भारतीय दूरसंचार विनियामक प्राधिकरण

Telecom Regulatory Authority of India

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

New Delhi, India
22nd April, 2025

Tower F, NBCC World Trade Centre, Nauroji Nagar, New Delhi-110029

CONTENTS

CHAPTER I
INTRODUCTION AND BACKGROUND

A. Introduction

1.1 The concept of machines exchanging information can be traced back to the early 20th century when communication was limited to wired transmissions. During this time, data could only be shared through physical cables, restricting the reach and flexibility of information exchange. However, significant progress was made in the late 1920s with the advent of telemetry, a technology that allowed sensors to transmit measurements to distant data processing systems via radio signals. This innovation eliminated the need for direct physical connections and paved the way for remote monitoring and control.

1.2 In the following years, advancements in telegraphy, telephony, radio, and television inspired the mathematician Claude Shannon to create a mathematical theory of information that introduced key concepts for reducing background noise and optimizing data transfer. Shannon's contributions not only enhanced the reliability of digital communication but also provided the theoretical foundation for modern M2M interactions, enabling seamless and efficient machine-based data exchange across various industries.

1.3 In the second half of the 20th century, caller ID and automatic meter readings became key milestones in machine-to-machine (M2M) communication, enabling automated data exchange without human intervention. These innovations paved the way for more advanced systems that could transmit data remotely and efficiently.

1.4 Kevin Ashton, the co-founder of the Auto-ID Center at the Massachusetts Institute of Technology (MIT), is credited with coining the term "Internet of Things" in 1999. Ashton introduced this concept while working at Procter & Gamble. To demonstrate its potential, he embedded a tiny RFID microchip in lipstick and an antenna in a shelf, creating a system that could track products remotely[1]. This innovation reduced costs and improved efficiency by leveraging the expanding public Internet. To explain this idea, Ashton coined the phrase "Internet of Things". Later, in an interview, he stated, "*In the twentieth century, computers were brains without senses—they only knew what we told them. That was a huge limitation: ... In the twenty-first century, because of the Internet of Things, computers can sense things for themselves.*[2]*"* Aston also said, *"The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so."*[3]

1.5 In the 21st century, the rapid expansion of cellular networks and wireless Internet greatly accelerated development of Internet of Things (IoT). Machines could now communicate seamlessly over vast distances, leading to widespread adoption of IoT in industries, smart cities, and everyday life.[4]

B. IoT and M2M

1.6 In June 2012, International Telecommunication Union (ITU)[5] released its recommendation on 'Overview of the Internet of Things'[6]. In the recommendation, ITU defined 'Internet of things (IoT)' as *"[a] global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*". In the recommendation, ITU depicted the technical overview of IoT through the following diagram:

[1] Source: Ashton, K. (2015). *How to Fly a Horse: The Secret History of Creation, Invention, and Discovery*. Anchor Books.

[2] Source: https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/%20

[3] Source: https://www.historyofinformation.com/detail.php?id=3411

[4] Source: https://www.ionos.com/digitalguide/server/know-how/what-is-machine-to-machine-communication-m2m/

[5] ITU is the United Nations specialized agency for digital technologies (ICTs). Source: https://www.itu.int/en/about/Pages/default.aspx

[6] Source: ITU's recommendation ITU-T Y.2060 (06/2012), accessible at URL: Y.2060 : Overview of the Internet of things (itu.int)

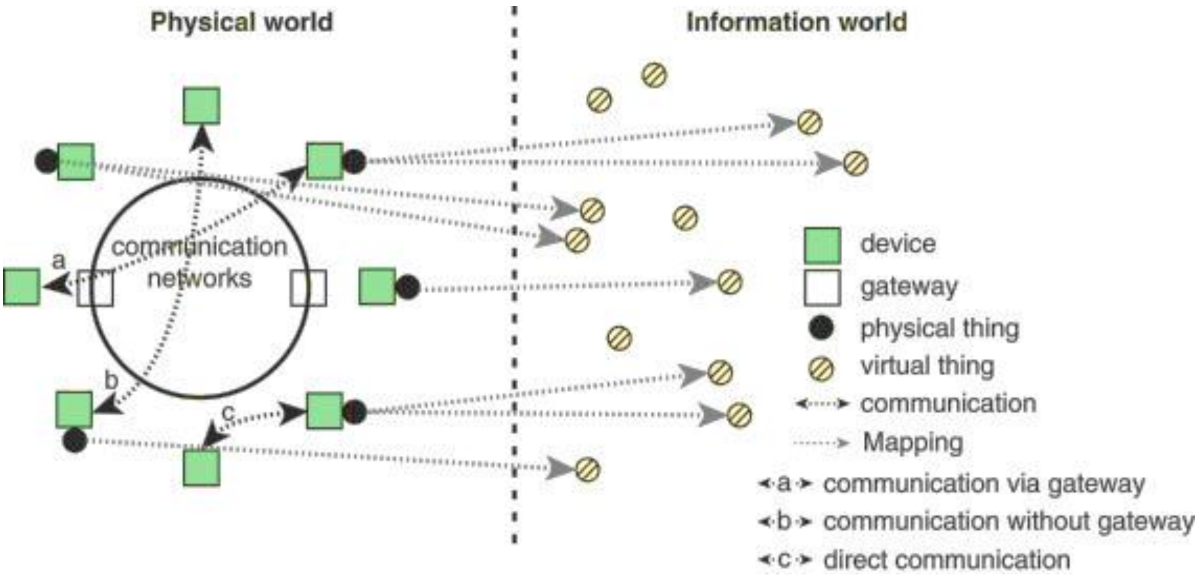


Figure 1.1: Technical Overview of IoT[7]

1.7 Notably, in the recommendation, ITU provided definitions of the terms 'device' and thing' as below:

"device: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing."

"thing: With regard to the Internet of things, this is an object of the physical world (physical thing) or the information world (virtual things), which is capable of being identified and integrated into communication networks".[8]

1.8 In the recommendation, ITU depicted the relations between devices and physical things through the following diagram:

[7] Source: ITU's recommendation ITU-T Y.2060 (06/2012), accessible at URL: Y.2060 : Overview of the Internet of things (itu.int)

[8] With respect to physical things and virtual things, ITU, through the recommendation ITU-T Y.2060 (06/2012), stated as below: *"Physical things exist in the physical world and are capable of being sensed, actuated and connected. Examples of physical things include the surrounding environment, industrial robots, goods and electrical equipment. Virtual things exist in the information world and are capable of being stored, processed and accessed. Example of virtual tings include multimedia content and application software."*

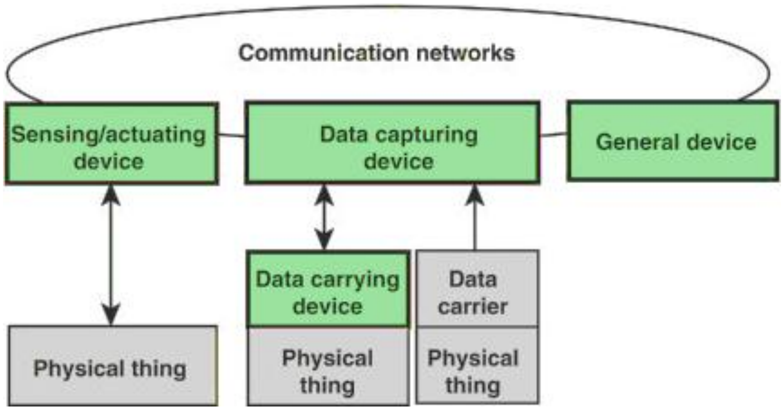


Figure 1.2: Types of devices and their relationship with physical things[9]

1.9 In India, Department of Telecommunications (DoT), Ministry of Communications, Government of India, in May 2015, issued National Telecom M2M Roadmap[10]. The roadmap defined M2M and IoT as below:

M2M*: "M2M, the acronym for Machine-to-Machine communication, is an emerging area in the field of telecom technologies. M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability. M2M uses a device (such as a sensor or meter) to capture an event, which is relayed through a network (wireless, wired or hybrid) to an application, that translates the captured event into meaningful information".*

IoT: *"IoT is connected network of embedded devices capable of having M2M communication without human intervention."*

1.10 In October 2023, Telecommunication Engineering Centre (TEC), a technical body of DoT, released a report[11] in which it provided a conceptual representation of M2M as below:

[9] Source: ITU's recommendation ITU-T Y.2060 (06/2012). In the recommendation, ITU observed that *"[t]he devices collect various kinds of information and provide it to the information and communication networks for further processing. Some devices also execute operations based on information received from the information and communication networks. … The communication networks transfer data captured by devices to applications and other devices, as well as instructions from applications to devices. The communication networks provide capabilities for reliable and efficient data transfer."*

[10] Source: https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

[11] Report on TEC initiatives in IoT domain_Oct 2023.pdf

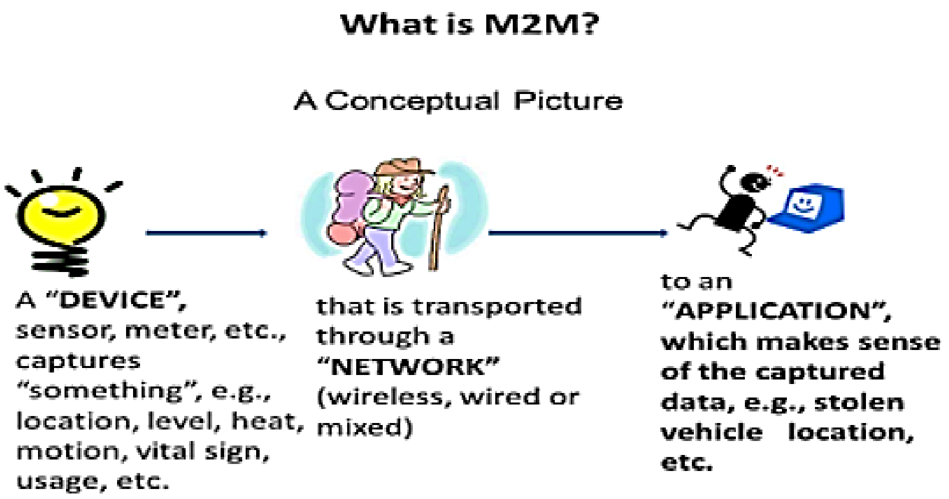

What is M2M?
A Conceptual Picture
A "DEVICE", sensor, meter, etc., captures "something", e.g., location, level, heat, motion, vital sign, usage, etc.
that is transported through a "NETWORK" (wireless, wired or mixed)
to an "APPLICATION", which makes sense of the captured data, e.g., stolen vehicle location, etc.

Figure 1.3: Conceptual representation of M2M[12]

C. M2M Ecosystem

1.11 The M2M ecosystem is entirely different from the standard telecommunication ecosystem. It is more diverse and involves multiple stakeholders. The oneM2M[13] has outlined the M2M ecosystem as below[14]:

(a) User (individual or company): Uses an M2M solution

(b) Application Service Provider: Provides an M2M application service, and operates M2M applications

(c) M2M Service Provider: Provides M2M services to Application Service Providers, and operates M2M common services

(d) Network Operator: Provides connectivity and related services for M2M Service Providers and operates an underlying network.

[12] Source: Report on TEC initiatives in IoT domain_Oct 2023.pdf

[13] oneM2M is a global partnership initiative of eight standards development organizations: ARIB (Japan), ATIS (North America), CCSA (China), ETSI (Europe), TIA (North America), TSDSI (India), TTA (Korea), and TTC (Japan) to develop specifications for Machine-to-Machine (M2M) communications systems and the Internet of Things (IoT).

[14] Source: https://www.onem2m.org/harmonization-m2m

D. Use Cases of M2M

1.12 M2M can enable applications and services across a broad range of vertical markets. To illustrate, a few verticals and related M2M applications are given below:

S. No.	Industry verticals	M2M applications
1	Automotive	Vehicle tracking, e-call, V2V & V2I applications, Traffic control, Navigation, Infotainment, Fleet management, Asset tracking, Manufacturing, Logistics, etc.
2	Utilities	Smart metering, Smart grid, Electric line monitoring, Gas/ Oil/ Water pipeline monitoring, etc.
3	Healthcare	e-health, Remote diagnostics, Medication reminders, Tele-medicine, wearable health devices, etc.
4	Safety and Surveillance	Women Safety Bands, Commercial and home security monitoring, Surveillance applications, Fire alarm, Police/medical alert, etc.
5	Financial	Point of sale (POS), ATM, Kiosk, Vending machines, Digital signage, and Handheld terminals, etc.
6	Public Safety	Highway, Bridge, Traffic management, Homeland security, Police, Fire, and Emergency services, etc.
7	Smart City	Intelligent transport System, Waste management, Street Light control system, Water distribution, Smart Parking, etc.
8	Agriculture	Remotely controlled irrigation pump, Remote Monitoring of Soil Data, etc.

Table 1.1: Examples of M2M applications

E. M2M Communication Technologies

1.13 Many communication technologies are used in the M2M/ IoT domain depending upon the requirements of applications such as coverage, power, quality of service (QoS) etc. Telecom Engineering Center (TEC), in its technical report on 'Communication Technologies in M2M/ IoT Domain' (2017)[15], identified the wireless technologies for M2M communication as below:

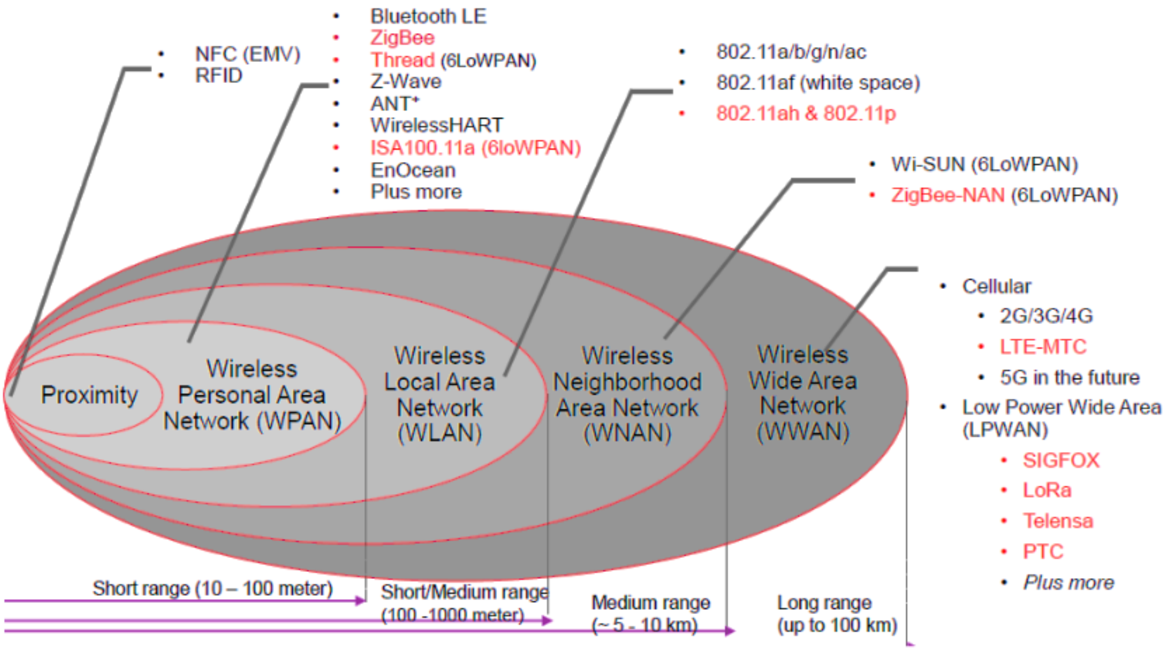

NFC (EMV)
RFID
Bluetooth LE
ZigBee
Thread (6LoWPAN)
Z-Wave
ANT+
WirelessHART
ISA100.11a (6loWPAN)
EnOcean
Plus more
802.11a/b/g/n/ac
802.11af (white space)
802.11ah & 802.11p
Wi-SUN (6LoWPAN)
ZigBee-NAN (6LoWPAN)
Cellular
2G/3G/4G
LTE-MTC
5G in the future
Low Power Wide Area (LPWAN)
SIGFOX
LoRa
Telensa
PTC
Plus more
Proximity
Wireless Personal Area Network (WPAN)
Wireless Local Area Network (WLAN)
Wireless Neighborhood Area Network (WNAN)
Wireless Wide Area Network (WWAN)
Short range (10 – 100 meter)
Short/Medium range (100 -1000 meter)
Medium range (~5 - 10 km)
Long range (up to 100 km)

Figure 1.4: Key wireless technologies for M2M communication[16]

1.14 In the afore-mentioned technical report, TEC mentioned that the wide area network (WAN) may also have wired technologies such as fixed line broadband, fiber to the home (FTTH) and power line communication (PLC).

1.15 In November 2021, TEC issued another technical report on 'Emerging Communication Technologies and Use cases in IoT Domain'[17]. In the technical

[15] Source: https://www.tec.gov.in/pdf/M2M/Communication%20Technologies%20in%20IoT%20domain.pdf

[16] Ibid

[17] Source: https://tec.gov.in/pdf/M2M/Emerging%20Communication%20Technologies%20&%20Use%20Cases%20in%20IoT%20domain.pdf

report, TEC also included 5G, Wi-Fi 6, Wi-Fi 6E, Wi-Fi HaLow[18], and Bluetooth Mesh[19] as key technologies for M2M communication.

1.16 Essentially, TEC, in its technical reports, has classified M2M communication technologies based on the range of communication. Typical ranges and typical M2M communication technologies for various types of networks are given below:

S. No.	Type of network	Typical range of communication	Examples of M2M communication technologies
1	Proximity	~ 1 m	NFC, RFID
2	Personal Area Network (PAN)	10 - 100 meter	Bluetooth, Zigbee, Thread, Z-wave, ANT, Wireless HART, ISA100.11a, EnOcean
3	Local Area Network (LAN)	100 - 1000 meter	802.11a/b/g/n/ac, 802.11af, 802.11ah and 802.11p
4	Neighborhood Area Network (NAN)	5 - 10 km	Wi-SUN, ZigBee-NAN
5	Wide Area Network (WAN)	Upto 100 km	Cellular (2G/ 3G/ 4G/ 5G) Wired technologies such as fixedline Broadband, FTTH and powerline communication LowPower Wide Area Network (LPWAN) technologies such as SIGFOX, LoRa, Telensa, PTC

Table 1.2: Features of typical networks for M2M

[18] Wi-Fi HaLow operates in spectrum below 1GHz with a typical range of 1 km. It is part of the Wi-Fi stack developed by Wi-Fi Alliance. Source: https://www.quectel.com/what-is-wi-fi-halow-iot

[19] Bluetooth Mesh is a computer mesh networking standard based on Bluetooth Low Energy that allows for many-to-many communication over Bluetooth radio.

1.17 A brief description of the technologies used for M2M communications is given in **Annexure II** of these recommendations.

F. Existing Regulatory Framework for M2M Communication Services in India

1.18 DoT has devised a three-tiered regulatory framework for M2M communication services in the country as outlined below:

S. No.	**Type(s) of networks for provisioning M2M communication services**	**License/ Registration required for operating the network(s)**	**Type of frequency spectrum**
1	Wireless Personal Area Network (WPAN), and Wireless Local Area Network (WLAN)[20]	Registration of WPAN/ WLAN Connectivity Provider for M2M Services	Unlicensed
2	Low Power Wide Area Network (LPWAN)[21]	M2M Authorization under Unified License	Unlicensed
3	Access network within a telecom circle/ Metro area[22] – cellular networks as well wireline networks	Access Service Authorization under Unified License and Unified Access Service License	Licensed

Table 1.3: The regulatory framework for M2M communication services in India

[20] The Guidelines for Registration Process of M2M Service Providers(M2MSP) & WPAN/WLAN Connectivity Providers for M2M Services define WPAN and WLAN as below:
"WPAN": A Personal Area Network (PAN) is a network used for data transmission among personal devices such as computers, phones, personal digital assistants, wearables, etc. Wireless PAN or WPANs can be used for communication among the personal devices (intra-personal communication), or for connecting to a higher-level network and the Internet (an uplink). Technologies used in PAN are Bluetooth, Z-Wave, ZigBee, RFID etc.
"WLAN" means a wireless network whereby a user can connect to a local area network (LAN) through a wireless (radio) connection, as an alternative to a wired local area network. An example of a Wireless LAN is Wi-Fi.

[21] As per the Unified License Agreement, "*LPWAN is type of WAN which provide wireless connectivity to low-power devices over large distance that is suited for M2M communication*". Source: https://dot.gov.in/sites/default/files/Compendium-UL-AGREEMENT%20updated%20up%20to%2031032024.pdf?download=1

[22] As per the Unified License Agreement, *"[t]he Access Service under Access Service authorization covers collection, carriage, transmission and delivery of voice and/or non-voice MESSAGES over Licensee's network in the designated Service Area. … The Licensee may provide access service, which could be on wireline and / or wireless media with full mobility, limited mobility and fixed wireless access".* The service areas for access service are telecom circles/ metro areas.

1.19 The present regulatory framework for the use of licensed and unlicensed spectrum for providing M2M communication services, may be summarized as below:

(a) M2M communication services using the unlicensed spectrum: The entities holding the 'M2M authorization under Unified License' may provide M2M communication services through the LPWAN[23] or equivalent technologies using unlicensed spectrum[24]. The entities holding the 'Registration of WPAN/ WLAN Connectivity Provider for M2M Services' are authorized to use WPAN/ WLAN technologies in the unlicensed spectrum to provide M2M communication services.

(b) M2M communication services using the licensed spectrum: The entities holding the Access Service authorization under Unified License or Unified Access Service License can obtain the licensed access spectrum from the DoT to provide wireless access services including M2M communication services. Various licensees holding the Access Service authorization under Unified License have obtained the access spectrum in the 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2300 MHz, 2500 MHz, 3300 MHz, and 26 GHz bands to provide wireless access services using GSM/ WCDMA/ LTE/ CDMA/ IMT-2020 technologies. They are permitted to use other technologies based on the standards approved by ITU/ TEC or any other International Standards Organization/ bodies[25].

1.20 As per the Unified License agreement, the Unified Licensees holding the Access Service authorizations can also provide M2M communication services through the LPWAN or equivalent technologies using the unlicensed spectrum. They may also provide WPAN/ WLAN connectivity in the unlicensed bands.

[23] LPWAN is an acronym of Low Power Wide Area Network.

[24] Source: https://dot.gov.in/sites/default/files/Compendium-UL-AGREEMENT%20updated%20up%20to%2031032024.pdf?download=1

[25] Source: https://dot.gov.in/sites/default/files/Notice%20Inviting%20Applications%202023-24.pdf

G. TRAI's Recommendation on Critical Services in the M2M Sector Dated 05.09.2017

1.21 On 05.09.2017, TRAI sent its recommendations[26] on 'Spectrum, Roaming and QoS Related Requirements in Machine-to-Machine (M2M) Communications' (hereinafter, also referred to as, "the Recommendations dated 05.09.2017") to DoT. TRAI, in the Recommendations dated 05.09.2017, made the following observations with respect to critical services in the M2M sector:

"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."

[26] The recommendations dated 05.09.2017 are available at the TRAI's website at the following URL: https://www.trai.gov.in/sites/default/files/2024-09/Recommendations_M2M_05092017_0.pdf

1.22 Based on the above observations, the Authority, through the M2M Recommendations of 2017, 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."*

H. DoT's Reference Dated 01.01.2024

1.23 Through a letter dated 01.01.2024 (**Annexure I**), the Department of Telecommunications (DoT), Ministry of Communications, Government of India sent a reference to Telecom Regulatory Authority of India (hereinafter, also referred to as "TRAI", or "the Authority") under the terms of section 11 of TRAI Act, 1997 (as amended). The reference is reproduced below:

"This has reference to the TRAI recommendation dated 05.09.2017 on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" which were accepted by the Government and same was conveyed vide letter No.4-16/2015-NT of March '20. (copy enclosed as Annexure I).

1.1. One of the recommendations of TRAI (Para 5.1 (g)) was with respect to identification of Critical Services in M2M sector. The same is reproduced here in under-

"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.

1.2 Government accepted the above recommendation with the following remarks: The deliberations converged into an agreement that critical services do require SLAs for effective delivery of services at a certain QoS as may be intended. Considering the scope and breadth of this potential issue, DoT will take up a detailed consultation with all stakeholders to comprehensively examine and identify critical services in this regard.

Considering the specific and critical needs of such services and taking into consideration of evolving technologies and needs, as the case may be, government shall declare any such service as critical from time to time.

1.3 In order to have a wider understanding of sectoral requirements of critical M2M *applications, an Inter-Ministerial Working Group (IMWG) was constituted in Nov. 19 to deliberate on all issues concerning critical M2M services. The aforesaid Working Group submitted its report in March 21. The IMWG recommended a list of 20 services to be classified as critical along with broad regulatory requirements for critical services. (Relevant excerpt of the IMWG Report is attached as Annexure-II).*

1.4 Subsequently, the guidelines for M2M Authorisations under UL and UL- VNO, M2M Service Provider Registration and Captive Non-Public Network (CNPN) License were issued by DoT in Jan, Feb, and June 2022 respectively.

1.5 Considering the introduction of aforesaid new license (UL-M2M) and registration policy, comments were solicited from all relevant stakeholders in the M2M/ IoT ecosystem (including keyline ministries, registered M2M Service Providers and other stakeholders) on the IMWG Report and SLA required for Critical Services. The list of stakeholders who have provided comments, is placed at Annexure-III.

2. Following points have emerged based on the comments received from various stakeholders necessitating a need to revisit and examine afresh the abovesaid recommendation-

I. Use of licensed spectrum may not be made mandatory for critical services/ sector, if the requisite Service Level Agreements (SLAs)/ Quality of Service (QoS) can be met through unlicensed spectrum. Many Startups/ companies are designing their model to operate in license-free band. 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. Further, the relationship between security of M2M services and these services operating on licensed spectrum was not cogent.

II. 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. Further, the SLA/ QOS framework along-with detailed regulatory requirement for the same may also be defined by respective concerned ministries/ regulatory bodies for different use cases (which are identified as critical) and implementing technologies may comply with the same.

III. A balanced approach of utilizing both licensed and unlicensed bands may be the *way forward to improve customer experience, drive innovation and increase affordability. Connectivity may be left to the discretion of the customer/ministries based on service parameters required for an application and not be enforced.*

IV. Critical M2M services may require robust, resilient, reliable, redundant and secure network. However, with the ever-growing interconnectivity of devices in the Internet of Things (IoT) and Machine-to-Machine (M2M) domains, it has now become crucial to ensure the security and trust worthiness of these devices. Therefore, bringing M2M/ IoT devices under the Trusted Source Trusted Product regulation, specifically mandating the procurement of M2M/ IoT devices for Critical Infrastructure Sectors, as defined in the National Critical Information Infrastructure Protection Centre (NCIIPC) regulations can significantly mitigate the threat landscape and enhance the security posture of critical infrastructure sectors rather than merely mandating provision of these services by connectivity providers using licensed spectrum.

3. Secondly, as per extant instructions, SIMs are non-transferable. A provision was introduced vide DoT instructions dated 16.05.18 to update the details of person to whom device is transferred in the database of the licensee (as intimated by M2MSP to the licensee) in case the devices with M2M SIM(s) are sold or transferred, However, there is no provision for change in the name of the owner of the M2M SIM.

3.1 Industry has requested to allow the transfer of ownership of M2M SIMs for the following scenarios:

i. Involving mergers, acquisitions, takeover of companies.

ii. For cases where 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.

iii. For cases where M2MSP is ceasing its operations or is filing for bankruptcy, etc. and the M2M SIMs are required to be either transferred to the new M2MSP or directly to the company where M2M SIMs are used/ deployed.

It is therefore necessary to examine the issue related to Transfer of ownership in case of M2M SIMs in view of situations narrated at 3.1 above.

4. Accordingly, TRAI is requested to provide reconsidered recommendations, as per provisions of Section 11 of the TRAI Act 1997 as amended from time to time on-

i. Identification of Critical Services in the M2M Sector *ii. Transfer of Ownership of M2M SIMs"*

1.24 Hereinafter, the afore-mentioned reference will also be referred to as "the Reference dated 01.01.2024".

1.25 Through a letter dated 12.01.2024, TRAI requested DoT to provide additional information with respect to the Reference dated 01.01.2024 including a clarification as to whether the list of 20 services, identified as critical by the IMWG, has been approved. In response, DoT provided requisite additional information and informed, *inter-alia*, that "*the list of 20 services, identified by the Inter-Ministerial Working Group (IMWG), doesn't have the approval of DoT*".

I. TRAI's Consultation Paper Dated 24.06.2024

1.26 In respect of the Reference dated 01.01.2024, the Authority issued a consultation paper on 'the Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs' on 24.06.2024 (hereinafter also referred to as "the Consultation Paper dated 24.06.2024") for soliciting comments of stakeholders on various issues related to the subject. Stakeholders' comments and counter-comments were invited on the Consultation Paper dated 24.06.2024 by 22.07.2024 and 05.08.2024 respectively. Upon request of a few stakeholders, the dates were extended to 19.08.2024 and 02.09.2024, respectively. In response, the Authority received 16 comments and one counter comment from stakeholders. The comments and counter comment received from stakeholders have been placed on the TRAI's website www.trai.gov.in. An online Open House Discussion (OHD) was held on 24.10.2024 with stakeholders through virtual mode.

J. Present Recommendations

1.27 Based on the comments and counter-comments received from stakeholders on the Consultation Paper dated 24.06.2024, and its further analysis, the Authority has arrived at the present recommendations. The recommendations comprise of three chapters. This chapter provides an introduction and background to the subject. Chapter II presents an analysis of the issues raised in the Consultation Paper dated 24.06.2024 considering comments and counter-comments received from stakeholders and the recommendations of the Authority thereon. Chapter III provides a summary of the recommendations of the Authority on the subject.

CHAPTER II
ANALYSIS OF ISSUES

2.1 This chapter presents an analysis of the issues raised in the Consultation Paper dated 24.06.2024 considering the comments and counter-comments received from stakeholders, and recommendations of the Authority thereon.

2.2 Through the Consultation Paper dated 24.06.2024, the Authority requested stakeholders to provide comments on the following broad issues:

(a) Need for a broad guiding framework for defining a service as critical M2M/ IoT service;

(b) Need for a review of the recommendation No. 5.1(g) of the TRAI's Recommendations of dated 05.09.2017;

(c) Need to bring M2M devices under the Trusted Source/ Trusted Product framework; and

(d) Need to establish a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs.

2.3 An analysis of the afore-mentioned issues based on the comments and counter-comments received from stakeholders is given below.

A. Need for a Broad Guiding Framework for Defining Critical M2M/ IoT Services

2.4 Through the Consultation Paper dated 24.06.2024, the Authority solicited comments on the following question:

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.

(1) Responses of Stakeholders on Q1

2.5 Broadly, two types of views have been received from stakeholders on Q1. While most stakeholders have opined that there is a need for a broad guiding framework for defining a service as critical M2M/ IoT service, a few other stakeholders have contended against it.

2.6 The stakeholders, who have opined that there is a need for a broad guiding framework for defining a service as critical M2M/ IoT service, have provided the following arguments in support of their viewpoint:

(a) A broad guiding framework for defining critical M2M/ IoT services is essential for mitigating risks and ensuring robust security measures in the rapidly expanding field. By establishing clear definitions and promoting collaborative development, safe and reliable operations of critical infrastructure and applications can be ensured.

(b) The adoption of IoT will increase significantly in future, especially in industrial automation and smart manufacturing. A guiding framework will ensure consistent and standardized criteria for what constitutes a critical M2M/ IoT service.

(c) M2M/ IoT services are being used in smart grids, remote surgery systems, autonomous vehicles and many industrial control systems used in critical infrastructure. Any malfunctioning of these services may lead to devastating consequences. A broad guiding framework for defining critical M2M/ IoT services will help the following:

(i) A clear definition may help establishing accountability of service providers and device manufacturers. Such a framework can ensure the implementation of appropriate security measures and contingency plans to minimize disruptions and vulnerabilities.

(ii) A standardized framework can promote consistency in security protocols, data formats, and communication standards.

(iii) Defining critical M2M/ IoT services allows for targeted risk assessments and mitigation strategies.

2.7 The stakeholders, who have opined that there is a need for a broad guiding framework for defining a service as critical M2M/ IoT service, have also suggested certain guiding principles for defining critical M2M/ IoT services as outlined below:

(a) Many stakeholders have suggested that the following classification should be considered for defining critical M2M/ IoT services:

(i) Services which support critical business services and infrastructure which are vital to national interests

(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 and environmental hazards to citizens

(b) A stakeholder has suggested that the framework for defining critical M2M/ IoT services should include the following considerations:

(i) Time sensitivity and latency: Services that must operate within stringent time constraints, where delays can lead to significant negative outcomes

(ii) Reliability and availability: Services that require near-constant uptime and resilience to disruptions

(iii) Data integrity and security: Services that require accurate, secure, and protected data flows

(iv) Safety and human impact: Services that can directly affect human health and safety

(v) Economic impact: Services that significantly affect economic activities or operational efficiencies

(vi) National Security: Services that are critical to national security, public order or essential public services

(vii) Scalability and flexibility: Services that require the ability to scale operations and adapt to increased reach and scope without compromising service quality

(c) Another stakeholder has suggested that the guiding framework should have the following criteria for defining a service as critical M2M/ IoT service:

(i) Life threatening: Smart medical devices, connected ambulances, telematics (AIS:140)

(ii) Business impacting: Smart metering, connected vehicles, car infotainment

(iii) Livelihood and employment: Smart water, smart agriculture, weather forecast for fishermen

(iv) Community services: Emergency response, dial ambulance, Call a TOW, smart cities, smart polling, smart parking

2.8 A stakeholder has proposed the following definition for critical services in the M2M/ IoT sector:

'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).'

2.9 A stakeholder has contended that the objective should be to ask the question contrarily (i.e. which are the M2M/ IoT services which can be accredited as non-critical?). It has argued that with high acceleration and penetration of M2M/ IoT, it is likely to intrude into every aspect of human and objects and possibly will become the critical back bone of any individual, object, industry, machine or service with cross-geographical cyber impacts; a few examples could be metering, automotive, health, energy, infrastructure, smart city, any nationally critical systems, home automation manufacturing 4.0, and access control; the technological advancement and peripheral use cases will continue to attract implementations and adaptations; therefore, the focus should be to regulate, standardize and securitize it from the beginning and continue to innovate and upgrade such measures to address prevalent, and anticipated challenges.

2.10 A stakeholder has opined that TRAI should recommend broad guidelines for defining a service as critical IoT/ M2M service, and respective departments/ ministries should define critical services/ applications along with the specific operational requirements which will be part of their regulatory domain.

2.11 On the other hand, a few stakeholders have contended that there is no need for a broad guiding framework for defining a service as critical M2M/ IoT service. A broad summary of the comments from such stakeholders is given below:

(a) There is no global example for the classification of IoT devices based on criticality of use case.

(b) A universal framework may not work as it may lead to increased costs, over-engineering, and delays where it is difficult to ascertain if the use case is critical or not. Instead, quality of service (QoS) and regulatory needs should be tailored to each use case.

(c) In the current scenario, the definition of critical services is very wide. Each domain or each sector may present a variety of use cases, and each may have its own specific needs. Therefore, it would not be possible to create a criticality framework for every use case in every industry/ domain when new use cases frequently emerge. QoS framework along with detailed regulatory requirements for specific needs are best understood by the consumer/ buyer of services. The criticality of M2M services in any domain/ sector should be decided based on the market requirement and criticality of any service should be use-case driven and should not be made applicable for the entire domain/ sector.

(2) Analysis w.r.t. the Issues Raised Through Q1

2.12 TRAI, through the Recommendation No. 5.1(g) of the Recommendations dated 05.09.2017, 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."* With respect to the said recommendation, DoT, through the reference dated 01.01.2024, conveyed to TRAI that *"Government accepted the above recommendation with the following remarks: The deliberations converged into an agreement that critical services do require SLAs for effective delivery of services at a certain QoS as may be intended. Considering the scope and breadth of this potential issue, DoT will take up a detailed consultation with all stakeholders to comprehensively examine and identify critical services in this regard.*

2.13 In this regard, the Government, in November 2019, constituted an Inter-Ministerial Working Group (IMWG) to have a wider understanding of the sectoral requirements of critical M2M applications. The IMWG furnished its report in March 2021 with the following key observations:

"

(a) Critical Internet of Things (IoT) is an emerging concept in IoT development that enables more efficient and innovative services across a wide range of industries by reliably meeting time-critical communication needs.

(b) Critical IoT addresses the time critical communication needs of individuals, enterprises, and public institutions. It is intended for time-critical applications that demand data delivery within a specified time duration with required guarantee (reliability) levels.

(c) Failure in a critical IoT system unlike with massive IoT, could lead to widespread systematic issues within a smart city, business, or infrastructure setting. Critical services thus require high QoS, ultra reliability, very low latency, very high availability alongwith accountability with requisite security."

2.14 In its report, the IMWG recommended that the following services should be classified as critical M2M/ IoT services:

"

i. Connected and Autonomous Cars/ three wheelers and two wheelers.

ii. Remote Surgery - 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 and Gas.

viii. Safety & Surveillance: State, Commercial and home security monitoring, Surveillance applications, Fire alarm, Police.

ix. Defense 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. Distribution Network of inflammable/ explosive articles.

xv. Chemical and Nuclear Industry.

xvi. Food Industry including Smart Cultivation, Storage and Public Distribution Systems.

xvii. Aviation - Remote radar systems.

xviii. Drone Communications including UAV-UAV, UAV-GCS and UAV- Network.

xix. Space and Research.

xx. Control network of Smart Cities."

2.15 Through the Reference dated 01.01.2024, DoT has informed that it solicited comments from all relevant stakeholders in the M2M/ IoT ecosystem including key line ministries, registered M2M Service Providers, and other stakeholders on the IMWG Report and SLA required for critical services. DoT has stated that based on the comments received from various stakeholders, <u>the following points have emerged which necessitate a need to revisit and examine afresh the TRAI's recommendation relating to critical services in M2M sector</u>:

"I. ….

II. 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. Further, the SLA/ QOS framework along-with detailed *regulatory requirement for the same may also be defined by respective concerned ministries/ regulatory bodies for different use cases (which are identified as critical) and implementing technologies may comply with the same.*

III. ...

IV. ..."

2.16 Keeping the above in view, the Authority, through the Consultation Paper dated 24.06.2024, solicited comments of stakeholders on the need for a broad guiding framework for defining a service as critical M2M/ IoT service. In response, most stakeholders have expressed a view that there is a need for a broad guiding framework for defining a service as critical M2M/ IoT service. The stakeholders have also suggested certain aspects which should be considered for defining critical M2M/ IoT services. A few stakeholders have, however, contended that there is no need for any guiding framework for defining a service as critical M2M/ IoT service.

2.17 While analyzing the comments of stakeholders on Q1, the Authority took note of the following aspects:

(a) Ericsson, in its white paper[27] on the Cellular Networks for Massive IoT (2016), made a distinction of massive IoT and critical IoT. In the white paper, Ericsson stated that "*[a]t one end of the scale, in Massive IoT applications – typically sensors that report to the cloud on a regular basis – the end-to-end cost must be low enough for the business case to make sense. Here, the requirement is for low-cost devices with low energy consumption and good coverage. At the other end of the scale, Critical IoT applications will have very high demands for reliability, availability and low latency*." In its white paper, Ericsson also depicted different requirements for massive IoT and critical IoT as below:

[27] Source: https://gsacom.com/paper/cellular-networks-for-massive-iot-ericsson-white-paper/

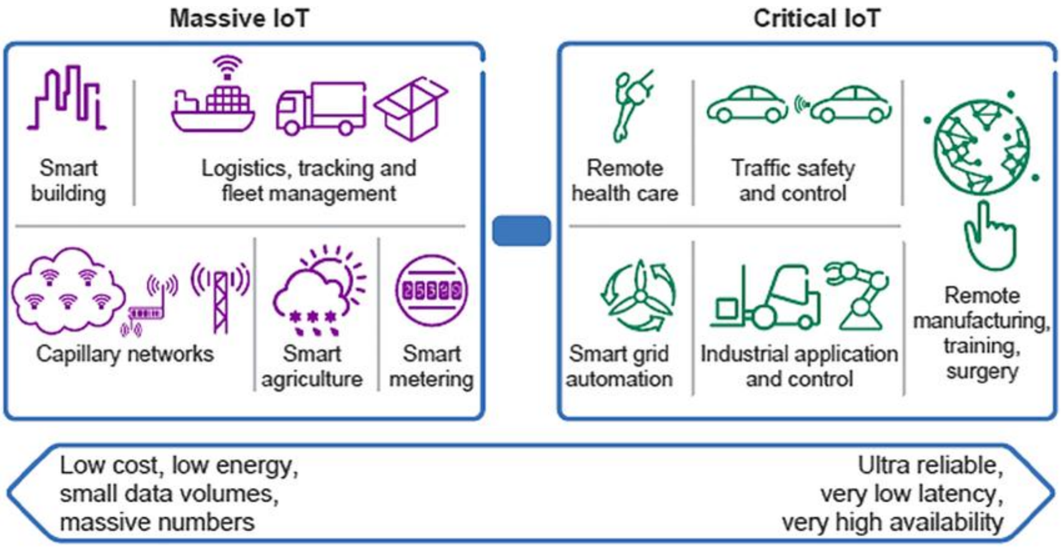

Massive IoT
Critical IoT
Smart building
Logistics, tracking and fleet management
Capillary networks
Smart agriculture
Smart metering
Remote health care
Traffic safety and control
Remote manufacturing, training, surgery
Smart grid automation
Industrial application and control
Low cost, low energy, small data volumes, massive numbers
Ultra reliable, very low latency, very high availability

Figure 2.1: Different requirements for communication networks for massive IoT and critical IoT applications[28]

(b) Nokia, in its article on 'Critical IoT vs. Massive IoT: How to spot the difference'[29], has compared the features of massive IoT and critical IoT. A summary of the article is given below:

(i) Massive IoT: Massive IoT defines applications with lots of endpoints that continuously serve little bits of data, mostly infrequently and to even remote locations. It involves applications that are low cost and low energy but with small data volumes in massive numbers that are reported regularly to the cloud. IoT sensors from billions of devices, objects, and machines communicate with one another, which require scalability and versatility. These devices are typically low cost and use very little energy individually but offer good coverage. Sufficient capacity is a core requirement for massive IoT along with network efficiency to connect potentially millions of devices. Massive IoT also requires long battery life and a wide coverage area. An example of massive IoT might be a temperature reading from a device in your home or business, or a simple on/ off application for a smart device or series of smart devices. Other

[28] Source: https://gsacom.com/paper/cellular-networks-for-massive-iot-ericsson-white-paper/

[29] Source: https://www.nokia.com/thought-leadership/articles/critical-massive-iot/

examples could include smart buildings, fleet management, smart meters, and smart agriculture.

(ii) Critical IoT: By contrast, critical IoT involves fewer endpoints that handle massive levels of data. Critical IoT will also require performance that can withstand harsh and remote environments, support for new manufacturing processes, scalability to support large-scale networks with thousands of controllers, robots, and machines, and security to protect end-point devices and networks against threats and attacks. One example of critical IoT is for industrial control of robotic machines and vehicles operating in hazardous locations. Failure in a critical IoT system, unlike with massive IoT, could lead to widespread systematic issues within a smart city, business, or infrastructure setting. Since applications such as traffic safety and control and managing power systems require time-sensitive information and precise positioning, reliability and low latency are vital. They must work without fail. If a connection goes down in a critical IoT system, there is far more at stake than if there were a massive IoT glitch. Imagine if a network issue occurs while a remote surgery is taking place, for example, or a boiler sensor malfunctions, causing tubes to overheat.

(c) As per PMRExpo, the future of critical communication will be defined by the IoT. Besides 5G, LPWAN technologies like NB-IoT, LTE-M, LoRa and MIOTY are technological pioneers for innovative IoT applications that require reliable connectivity. Critical IoT makes many applications possible, including: (i) industrial robotics, (ii) automated guided vehicle systems in networked factories, (iii) autonomous vehicles, and (iv) remote monitoring and control. The requirements for critical IoT are extremely high. The systems must also function reliably under extreme conditions and be scalable in order to support networks with thousands of control systems, robots, and machines. Besides, they must be secure, to protect terminals and networks from threats and attacks.[30]

[30] Source: https://www.pmrexpo.com/en/trade-fair/industries-thematic-areas/critical-iot/

(d) Ericsson Technology Review article[31] on 'Critical IoT connectivity: Ideal for time-critical communications' (2020) mentions that critical IoT addresses the time-critical communication needs of individuals, enterprises, and public institutions. It is intended for time-critical applications that demand data delivery within a specified time duration with required guarantee (reliability) levels, such as data delivery within 50 milli second with 99.9 percent likelihood (reliability).

2.18 At present, IoT/ M2M ecosystem is at an early growth stage of its lifecycle[32]. As the IoT/ M2M ecosystem matures, and thereby, gains user confidence, more and more services will be delivered to individuals, enterprises, and public institutions by using IoT. Many of such services will be critical in nature, and therefore, would require to be delivered by using critical IoT, i.e. ultra-reliable low-latency M2M connectivity with very high availability.

2.19 As critical IoT will be used for delivering services of critical importance, the Authority is of the view that the identification of services as critical IoT service requires to be done well in advance. The identification of a service as critical IoT service will enable user agencies to enter into suitable service level agreements (SLAs) with telecom service providers. Through the SLAs, the telecom service providers may be held accountable for ensuring that the M2M connectivity provided by them meets the requisite telecommunication service performance parameters (such as latency, reliability, and availability) which are sacrosanct for the successful operation of the concerned critical IoT service.

2.20 At this stage, the Authority also took note that Section 22(3) of the Telecommunications Act, 2023[33] provides that *"[t]he Central Government may, by notification in the Official Gazette, declare any telecommunication network, or part*

[31] Source: https://www.ericsson.com/4ac68c/assets/local/reports-papers/ericsson-technology-review/docs/2020/critical-iot-connectivity.pdf

[32] According to IoT Analytics, globally, there were 16.6 billion connected IoT devices in 2023, which are estimated to grow to 40 billion by 2030.

[33] Source: https://dot.gov.in/sites/default/files/Telecommunications%20Act%202023_1.pdf?download=1

thereof, as Critical Telecommunication Infrastructure, disruption of which shall have debilitating impact on national security, economy, public health or safety."

2.21 Considering the comments of stakeholders and its further analysis, the Authority is of the view that it would be appropriate to classify any service (application) as a 'critical IoT service' if it possesses the following attributes:

(a) The service demands ultra-reliable low-latency M2M connectivity with very high availability; and

(b) Any disruption of the M2M connectivity used for delivering the service will have a debilitating impact on national security, economy, public health, or public safety.

2.22 The Authority is of the view that the identification of a service as a critical IoT service would essentially be an involved exercise requiring numerous sector-specific and application-specific insights; therefore, concerned ministries/ regulatory bodies (in consultation with DoT) would be the best fit agencies for making such an identification. As more and more services will progressively be delivered using critical IoT, the broad guiding framework, outlined in the preceding paragraph, would enable the concerned ministries and regulatory bodies to define a service as critical M2M/ IoT service, as and when the need for such an identification arises.

2.23 As each domain/ sector will have both critical as well as non-critical services (applications) within it, it would be important to carefully identify the critical IoT services (applications) within a domain/ sector. This would also be necessary to avoid any over-kill, else even non-critical IoT services would be unduly burdened with stringent service performance benchmarks, and thereby, excess costs. Accordingly, the Authority is of the view that the identification of critical IoT requires to be done at the service (application) level rather than at the domain/ sector level.

2.24 Considering that more and more use cases and applications will emerge, any IoT service should be treated as a non-critical IoT service unless it is identified and notified as a critical IoT service.

2.25 As the classification of critical IoT services would essentially be a *de-novo* exercise, the Authority is of the view that it would be desirable that DoT devises an institutional mechanism for the assistance of concerned ministries/ regulatory bodies; the proposed institutional mechanism may include, *inter-alia*, the following aspects:

(a) The classification of critical IoT services of each domain/ sector should be done by a standing committee comprising of one or more officers nominated by the ministry/ regulatory body concerned and an officer nominated by DoT.

(b) DoT should establish an online repository of all critical IoT services (sector-wise), which should be accessible to the general public.

B. Should critical services in the M2M sector be permitted to be provided by using unlicensed spectrum as well?

2.26 Through the Consultation Paper dated 24.06.2024, the Authority solicited comments on the following question:

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.

(1) Responses of Stakeholders on Q2

2.27 Two types of views have been received from stakeholders on Q2. While many stakeholders have opined that critical services in the M2M sector should be permitted to be provided by using the unlicensed spectrum as well, many other stakeholders have contended that the earlier recommendation of TRAI that critical services in the M2M sector should be mandated to be provided only by connectivity providers using the licensed spectrum does not require a review.

2.28 Many stakeholders have opined that TRAI's earlier recommendation that critical services in the M2M sector should be mandated to be provided only by connectivity providers using the licensed spectrum requires a review. They have suggested that critical services in the M2M sector should be permitted to be provided by using the unlicensed spectrum as well. A broad summary of comments from such stakeholders is given below:

(a) The assumption of ensuring QoS through the licensed spectrum is over-simplification of facts. In India, unreliable coverage of cellular networks is also a fact. Cellular networks find it difficult to penetrate the walls at higher frequencies which are used in new generation cellular mobile networks. Smart devices installed in basements and inside the houses may find it difficult to connect to cellular mobile networks. The existing QoS requirements for the licensed spectrum may not necessarily match the QoS requirement for critical M2M services, whereas QoS can be reinforced more easily through Low Power Wide Area Networks (LPWANs). Due to technological developments and availability of additional unlicensed spectrum, both licensed and unlicensed spectrum offer a matching level of reliability and QoS. Critical M2M services, such as those used in healthcare, emergency services, and industrial automation, requiring uninterrupted and highly reliable communications can also be permitted on the unlicensed spectrum.

(b) Use of technology must be left on to the market forces and innovators. Any technology, which complies with the SLA/ QoS framework laid down by the concerned ministry/ sector regulator and meets regulatory requirements, should be permitted for the provision of critical M2M/ IoT services. IoT devices need stable connectivity for which innovators are using non-cellular technologies like, 6LoWPAN, Zigbee, Thread, Wireless HART etc. Enforcing the provision of critical services through licensed bands only by licensed telecom service providers may hamper the growth of the market as well as market driven research and development (R&D), startups, and smaller companies. Operational costs and upfront costs of devices also play an important role in making a choice between various technologies, and hence, market forces shall adopt the technologies based on their own requirements.

(c) A balanced approach of utilizing both licensed and unlicensed frequency spectrum in many scenarios is the best way to achieve improved customer experience, drive innovation and increase affordability.

(d) Any approach towards 'digital transformation' should be technology-agnostic rather than prescribing any specific technology/ spectrum band to support the use cases in M2M/ IoT domain. LPWAN-based networks (such as LoRa WAN) can support various use cases in different economic and social verticals including critical IoT services. Hence, along with 4G and 5G, other alternate technologies such as LPWAN-based networks should be equally considered and made part of any roadmap of DoT for critical IoT services.

(e) There are no global practices which identify and segregate critical IoT services to be provided only on the licensed spectrum. Globally, all low bandwidth IoT applications are catered by both LPWAN-based connectivity providers as well as mobile network operators (MNOs), while high bandwidth applications can be catered only by MNOs. For a user of any IoT applications, all such applications would be critical only and therefore, the mandate to obtain the licensed spectrum to offer the critical IoT/ M2M services would make the entire business model of Lora WAN-based M2M/ IoT services commercially unviable.

(f) Due to enhancements in unlicensed technologies, such technologies now provide security controls, essential for critical M2M services. Both licensed and unlicensed spectrum offer the same level of risk of unauthorized access and security breaches. Critical services do need robust security measures to prevent data theft, hacking, and other cyber threats and these can be implemented irrespective of the type of spectrum.

(g) Allowing critical M2M services on the unlicensed spectrum could foster innovation and reduce costs. It could lower entry barriers for new players and encourage the development of new technologies and business models. Trusted Source and Trusted Product regulations can better mitigate security threats than simply using the licensed spectrum.

2.29 A broad summary of comments received from stakeholders who have contended that the earlier recommendation of TRAI that *critical services in the M2M sector should* *be mandated to be provided only by connectivity providers using licensed spectrum* does not require a review is given below:

(a) 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.

(b) The usage of the 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.

(c) Critical IoT services often handle sensitive data and require robust security measures. The licensed spectrum provides a more secure environment, as it is less susceptible to unauthorized access and interference compared to the unlicensed spectrum. This is particularly important for applications in sectors such as healthcare, finance, and public safety.

(d) Critical services often rely on a resilient infrastructure that can withstand various challenges, including natural disasters and cyber threats. The licensed spectrum supports the development of robust networks that can provide the necessary redundancy and reliability for critical applications.

(e) The Government has administrative control over the licensed connectivity providers. Also, in the case of licensed telecom service providers (TSPs), the QoS parameters are measurable and enforceable. On the contrary, devices and applications using the 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 the critical public infrastructure.

(f) Considering the nature of critical IoT/ M2M services, such services should be given only through the licensed spectrum, else unlicensed spectrum holders should also be brought under similar licensing and regulatory framework as is applicable to licensed telecom service providers (TSPs). 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 as well.

(g) The issue of licensed spectrum versus unlicensed spectrum is not so much an issue of QoS and SLA. It is rather about an 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 communication networks and services. The licensed TSPs acquiring the licensed spectrum are obligated to ensure security measures in parallel.

(2) Analysis w.r.t. the Issues Raised Through Q2

2.30 Through the Recommendation No. 5.1(g) of the Recommendations dated 05.09.2017, TRAI recommended, *inter-alia*, that *"Government, through DoT, should identify critical services in M2M sector and <u>these services should be mandated to be provided only by connectivity providers using licensed spectrum</u>."* In this regard, through the Reference dated 01.01.2024, DoT has conveyed, *inter-alia*, that *"[f]ollowing points have emerged based on the comments received from various stakeholders necessitating a need to revisit and examine afresh the abovesaid recommendation*:

"I. Use of licensed spectrum may not be made mandatory for critical services/ sector, if the requisite Service Level Agreements (SLAs)/ Quality of Service (QoS) can be met through unlicensed spectrum. Many Startups/ companies are designing their model to operate in license-free band. 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. Further, the relationship between security of M2M services and these services operating on licensed spectrum was not cogent.

II. 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. Further, the SLA/ QOS framework along-with detailed regulatory requirement for the same may also be defined by respective concerned ministries/ regulatory bodies for different use cases (which are identified as critical) and implementing technologies may comply with the same.

III. A balanced approach of utilizing both licensed and unlicensed bands may be the way forward to improve customer experience, drive innovation and increase affordability. Connectivity may be left to the discretion of the customer/ ministries based on service parameters required for an application and not be enforced.

IV. Critical M2M services may require robust, resilient, reliable, redundant and secure network. However, with the ever-growing interconnectivity of devices in the Internet of Things (IoT) and Machine-to-Machine (M2M) domains, it has now become crucial to ensure the security and trust worthiness of these devices. Therefore, bringing M2M/ IoT devices under the Trusted Source Trusted Product regulation, specifically mandating the procurement of M2M/ IoT devices for Critical Infrastructure Sectors, as defined in the National Critical Information Infrastructure Protection Centre (NCIIPC) regulations can significantly mitigate the threat landscape and enhance the security posture of critical infrastructure sectors rather than merely mandating provision of these services by connectivity providers using licensed spectrum."

2.31 In view of the above, the Authority, through the Consultation Paper dated 24.06.2024, solicited comments of stakeholders on the need for a review of its earlier recommendation that *critical services in M2M sector should be mandated to be provided only by connectivity providers using licensed spectrum.* In response, stakeholders have provided a mixed response. While many stakeholders have opined that critical services in the M2M sector should be permitted to be provided by using unlicensed spectrum as well, many other stakeholders have contended that the earlier recommendation of TRAI that *critical services in the M2M sector should be mandated to be provided only by connectivity providers using licensed spectrum* does not require a review.

2.32 The Authority notes that with the passage of time, many technologies have emerged for M2M communications. While 3GPP based cellular mobile technologies were developed initially for person-to-person (P2P) communications and have later adapted themselves for M2M communications as well, many other technologies such as RFID, Bluetooth, Zigbee, Thread, Z-wave, ANT, 6LoWAN, WI-SUN, Wi-Fi, LoRa, SIGFOX have been developed mainly for M2M communications. While 3GPP-based cellular mobile technologies operate mainly on the licensed spectrum, other technologies such as RFID, Bluetooth, Zigbee, Thread, Z-wave, ANT, 6LoWAN, WI-SUN, Wi-Fi, LoRa, SIGFOX operate mainly on the unlicensed spectrum.

2.33 Many of the M2M communication technologies have been developed keeping in mind distinct use cases, and therefore, they possess unique service performance characteristics. In terms of the coverage distance, the present-day M2M communication technologies can be classified into four broad categories viz. Personal Area Network (PAN), Local Area Network (LAN), Low Power Wide Area Network (LPWAN) and Wide Area Network (WAN). The following figure depicts a matrix representation of M2M communication technologies in terms of coverage distance and data rate[34]:

[34] Source: https://ieeexplore.ieee.org/document/9848798

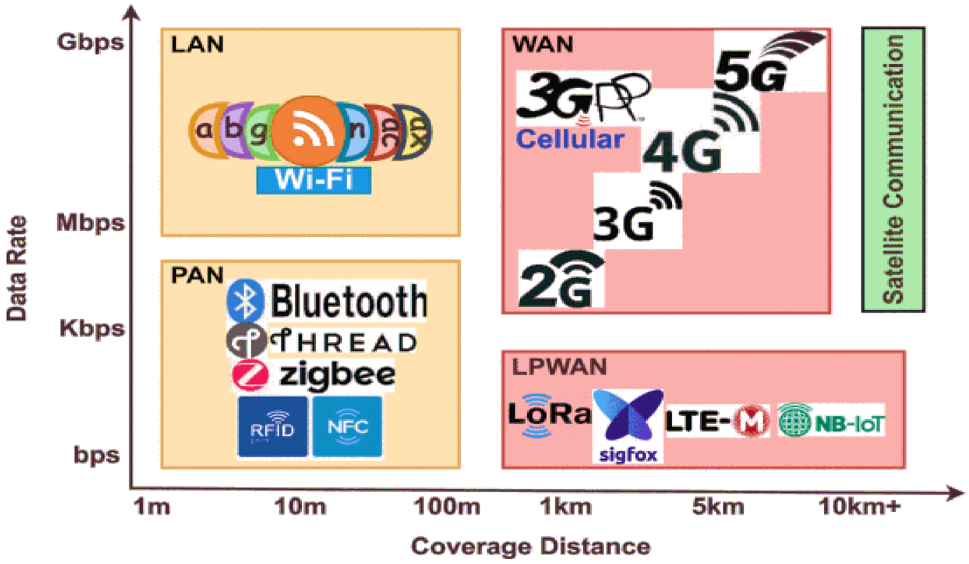


Figure 2.2: Comparative analysis of various M2M communication technologies[35]

2.34 The battery life of IoT devices is also a crucial aspect of the system design, as it determines the performance and efficiency of IoT devices. IoT devices are often installed in remote and hard-to-reach locations, where replacing or recharging the batteries can be difficult. For mission-critical applications, longer battery life is essential to prevent device failure and its consequences.[36] For these reasons, M2M communication technologies are designed to extend battery life for resource-constrained IoT devices (power efficiency).

2.35 Another important consideration for M2M communication technologies is their ability to communicate seamlessly in closed rooms with thick walls, more particularly in basements, as IoT devices in many use cases are deployed in such environments also.

2.36 The perusal of the present-day M2M communication technologies suggests that each of these technologies have their own strengths and weaknesses in terms of service performance parameters such as coverage, data rate, latency, reliability, availability, power efficiency. Besides, the overall cost of connectivity (i.e. cost of deployment, operation and maintenance of the IoT system) under various M2M communication

[35] Source: https://ieeexplore.ieee.org/document/9848798

[36] Source: https://www.powerelectronicsnews.com/battery-life-measurement-and-design-considerations-for-your-new-iot-device/

technologies differs vastly. As each IoT application demands specific service performance parameters for its successful operation, the user agencies, generally, evaluate both technological and financial aspects of various M2M communication technologies and choose the best fitting M2M communication technology for their IoT applications.

2.37 Ericsson, in its Report[37] on 'Critical IoT connectivity - Ideal for time critical communications' (June 2020), outlines that the service performance parameters such as the latency of critical IoT differ widely from one use case to another. An extract of the report is given below:

"Critical IoT addresses the time critical communication needs of individuals, enterprises and public institutions. …

The majority of time-critical use cases can be classified into the following four use case families:

⟫ Industrial control

⟫ Mobility automation

⟫ Remote control

⟫Real-time media

Each family is relevant for multiple industries and includes a wide range of use cases with more or less stringent time-critical requirements, …

Furthermore, there are three main network deployment scenarios depending on the coverage needs of time-critical services in different industries:

⟫ Local area

⟫ Confined wide area

⟫ General wide area

Local-area deployment includes both indoor and outdoor coverage for a small geographical area such as a port, farm, factory, mine or hospital. Confined wide-area deployment is for a predefined geographical area – along a highway, between certain electrical substations, or within a city center, for example. General wide-area

[37] Source: https://www.ericsson.com/4ac68c/assets/local/reports-papers/ericsson-technology-review/docs/2020/critical-iot-connectivity.pdf

deployment is about serving devices virtually anywhere. Common to all time-critical use cases is the fact that the communication service requirements depend on the dynamics of the use case and the application implementation. A highly dynamic system requires faster control with shorter roundtrip times (RTTs), while a slower control loop is sufficient for a system that operates more slowly. Various factors – such as device processing capabilities, the processing split between the device and the application server, the application's ability to extrapolate and predict data in case of missing packets, rate adaptivity and which codecs are used – impact both the application RTT and the latency requirements on the communication network."[38]

2.38 As outlined in para 2.32 above, both types of spectrums viz. licensed spectrum and unlicensed spectrum are used for M2M communications. In the consultation process, many stakeholders have asserted that owing to technological developments and availability of additional unlicensed spectrum, both licensed and unlicensed spectrum offer a matching level of reliability and QoS; therefore, the use of licensed spectrum should not be made mandatory if the requisite service performance parameters can be met through the unlicensed spectrum; the approach should be technology-agnostic; The use of both licensed and unlicensed spectrum for M2M communication in critical IoT services may be the way forward. Contrarily, many other stakeholders have suggested that only licensed spectrum should be used for the delivery of critical

[38] The report also provides the following description w.r.t. the varying degree of time-criticality of various critical IoT use cases:
"Mobility automation refers to the automation of control loops for mobile vehicles and robots. Examples of the least time-critical use cases in this category include the relatively self-sufficient automated guided vehicles (AGVs) equipped with advanced on-board sensors that are used for transportation in ports and mines. Infrastructure assisted vehicles such as fast-moving AGVs in a warehouse and collaborative maneuvering on public roads are examples of more time-critical mobility automation use cases, while the collaborative mobile robots used in flexible production cells represent an even higher degree of time-criticality.
Remote control refers to the remote control of equipment by humans. The ability to remotely control equipment is an important step in the evolution toward autonomous vehicles (to take temporary control of a driverless bus in scenarios not covered by its own automation functions) and for flying drones beyond visual line-of-sight. Remote control can also improve work environments and productivity by moving humans out of inconvenient or hazardous environments – remote-controlled mining equipment [5] is one example. Such solutions also offer the benefit of providing enterprises with access to a broader workforce.
The communication service requirements for remote control depend on how fast the remote environment changes, the required precision of the task and the required QoE. Control-loop latency and audio/video quality are important factors for QoE and the ergonomics for the remote operator. Haptic feedback and augmented reality (AR) can be used to further improve the operator QoE and task precision, and will make the acceptable latencies even stricter. Real-time media comprises use cases where media is produced and consumed in real time, and delays have a negative impact on QoE. Mobile applications for gaming and entertainment, including AR and virtual reality (VR), are common, with processing and rendering done locally in the device. Time-critical communication will make it possible to offload parts of the processing and rendering to the cloud [6], thereby improving the user experience and enabling the use of more lightweight devices (head-mounted, for example). Time-critical communication can enable cloud gaming over cellular networks as well as new applications in sectors such as manufacturing, education, health care and public safety. It is expected to drive more widespread use of mobile AR and VR. Advanced media production (such as real-time production of live performances) with its strict delay and synchronization requirements, is another area where time-critical communication can enable new use cases."
Source:
https://www.ericsson.com/4ac68c/assets/local/reports-papers/ericsson-technology-review/docs/2020/critical-iot-connectivity.pdf

IoT services as it provides exclusive access to operators, which significantly reduces the risk of interference from other users. One of the stakeholders, who is of the view that critical IoT services should be provided by using only licensed spectrum, has also mentioned that the issue of licensed spectrum versus unlicensed spectrum is not so much an issue of QoS and SLA; it is rather about an 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.

2.39 As far as the issue of IoT security is concerned, the Authority has taken up this issue while dealing with Q3 in the following section.

2.40 The above discussion may be summed up as below:

(a) Critical IoT applications require stringent service performance. However, these requirements differ significantly from one application to another.

(b) Various M2M communication technologies available today differ substantially from one another in terms of service performance and overall cost to the customer.

(c) Not only the licensed spectrum (which is mainly used in 3GPP based cellular mobile networks in India) but also the unlicensed spectrum (which is mainly used in the networks other than 3GPP based cellular mobile networks in India) can serve critical IoT applications.

2.41 In light of the above, the Authority is of the view that it would be prudent for a user agency implementing a critical IoT service to evaluate technological and financial aspects of various M2M communication technologies running on the licensed spectrum, M2M communication technologies running on the unlicensed spectrum, and wireline M2M communication technologies and choose the M2M communication technology for its critical IoT application, which is optimum from the standpoint of service performance and cost.

2.42 It is noteworthy that the Inter-Ministerial Working Group (IMWG) constituted to identify critical services in M2M sector had commented, *inter-alia*, that *"[d]etailed regulatory requirements for these critical services shall be issued by respective ministries/ regulatory bodies"*

2.43 In light of the above, the Authority reviewed the recommendation No. 5.1(g) of the recommendations dated 05.09.2017 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*". Based on a careful consideration of the factual matrix, the Authority is of the view that this recommendation requires a modification.

2.44 As far as the first part of the above recommendation [*Government, through DoT, should identify critical services in M2M sector]* is concerned, the Authority has already expressed a view that the classification of critical IoT services of a particular domain/ sector should be done by the concerned ministry/ regulatory body (in consultation with DoT) based on a pre-defined criterion. With respect to the second part of the above recommendation [*these services should be mandated to be provided only by connectivity providers using licensed spectrum],* the Authority is of the considered view that it would be appropriate to permit the provision of critical IoT services by using any M2M communication technology regardless of the consideration that it uses licensed spectrum or not as long as it meets the requisite service performance benchmarks.

2.45 Based on the comments of stakeholders on Q1 and Q2 and the foregoing analysis, the Authority makes the following recommendation:

Earlier, through the recommendation No 5.1 (g) of the recommendations on Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017, TRAI 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".* Based on a review of this recommendation, the Authority recommends as below:**

(a) A service (application) should be classified as a 'critical IoT service' if it passes the following twin tests:

(i) Whether the service (application) demands ultra-reliable low-latency M2M connectivity with very high availability?

(ii) Whether any disruption of the M2M connectivity used for delivering the service (application) will have a debilitating impact on national security, economy, public health, or public safety?

(b) Instead of classifying an entire domain/ sector as a critical IoT sector, specific IoT services (applications) within the domain/ sector should be classified as critical IoT services.

(c) The classification of critical IoT services of a particular domain/ sector should be done by the ministry/ regulatory body concerned in consultation with DoT.

(d) Any IoT service should be treated as a non-critical IoT service unless it is identified and notified as a critical IoT service.

(e) For the classification of critical IoT services, DoT should devise an institutional mechanism for the assistance of concerned ministries/ regulatory bodies. The institutional mechanism may include the following aspects:

(i) The classification of critical IoT services of each domain/ sector should be done on the basis of the recommendations of a standing committee comprising of one or more officers nominated by the ministry/ regulatory body concerned and an officer nominated by DoT. The standing committees should also recommend service performance benchmarks (such as latency, reliability, availability etc.) for each critical IoT service.

(ii) After considering the standing committee's recommendations, the concerned ministry/ regulatory body should notify the regulatory requirements including the telecommunication

service performance benchmarks (such as latency, reliability, availability etc.) for each critical IoT service separately.

(iii) DoT, as the nodal department, should establish an online repository of sector-wise critical IoT services and corresponding regulatory requirements including telecommunication service performance benchmarks, as prescribed by the concerned ministries/ regulatory bodies. The online repository should be accessible to the general public.

(f) Any wireless M2M communication technology (utilizing unlicensed spectrum, or licensed spectrum) or wired M2M communication technology should be permitted to be used for the provision of critical IoT services if it meets the prescribed service performance benchmarks. The choice for M2M communication technologies may be exercised by user agencies based on their techno-commercial considerations.

C. Security of IoT/ M2M Devices

2.46 Through the Consultation Paper dated 24.06.2024, the Authority solicited comments from stakeholders on the following question:

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.

(1) Responses of Stakeholders on Q3

2.47 In response to the afore-mentioned question, broadly three types of views have been received from stakeholders, as outlined below:

(a) View-1: All IoT/ M2M devices should be brought under the Trusted Source/ Trusted Product framework.

(b) View-2: Only M2M devices used for critical IoT/ M2M services should be brought under the Trusted Source/ Trusted Product framework.

(c) View-3: There is no need to bring IoT/ M2M devices under the Trusted Source/ Trusted Product framework.

2.48 A summary of the comments of the stakeholders who have opined that all M2M devices to be used in India should be brought under the Trusted Source/ Trusted Product framework is given below:

(a) With the increasing prevalence of cyber threats, it requires to be ensured that all M2M devices adhere to stringent security standards. Ensuring that these devices come from trusted sources can mitigate risks associated with compromised hardware or software, reducing vulnerabilities to cyber-attacks.

(b) The inclusion of M2M devices under the trusted framework will help verify the origin of devices and their components, reducing the risk of supply chain attacks where malicious actors could introduce compromised devices. It will create accountability among vendors, ensuring that they maintain high standards throughout their production processes.

(c) All M2M devices to be used in India should be under the trusted source framework to bring in standardization and to allow interoperability with other countries. The trusted framework for M2M devices can ensure that such devices comply with national and international regulations and standards, promoting a safer and more standardized technological environment.

2.49 One of the stakeholders who have supported inclusion of M2M devices under the Trusted Source/ Trusted Product framework, has stated that public sector (utilities, traffic, security, etc.) should be under a regulatory framework for added security. The non-public sector M2M devices (i.e. home automation and management, automobiles, consumer electronics, etc.) using unlicensed spectrum should be under much lighter regulatory control if at all.

2.50 A summary of the comments of the stakeholders who have suggested that all M2M devices to be used for critical IoT/ M2M services in India should be brought under the Trusted Source/ Trusted Product framework is given below:

(a) Though the standardization of devices and applications is important for IoT applications for scalability, it would be extremely important for all critical IoT applications in future as they may need to securely share data with multiple government and private agencies and other applications.

(b) For the identified critical IoT devices, all aspects need to be secured including device, application and connectivity as any unsecured elements may open the path for hackers to make backdoor entry and potentially disrupt the critical services.

2.51 A few stakeholders who have suggested that all M2M devices to be used for critical IoT/ M2M services in India should be brought under the Trusted Source/ Trusted Product framework have contended that while the licensed telecom service providers have to comply with the Trusted Source/ Trusted Product framework even for the communication devices operating on unlicensed spectrum (e.g. Wi-Fi routers and GPON devices), the unlicensed entities operating on a large-scale telecommunication network and connected to public resources are not required to comply with any of the security obligations. This makes the systems operating on the unlicensed spectrum more vulnerable than the systems using the licensed spectrum. In order to prevent significant security breaches in critical telecommunication infrastructure and to protect national security, the same security responsibilities should be imposed on such systems as well.

2.52 A summary of the comments from the stakeholders who have opposed bringing the M2M devices under the Trusted Source/ Trusted Product framework is given below:

(a) Coverage of M2M/ IoT services will require huge numbers of different types of devices as it will be used across many sectors/ verticals. Putting the requirement to bring all M2M devices under the Trusted Source/ Trusted Product framework will be a humongous task and further delay the uptake of M2M services in India.

(b) Performance and reliability are determined by the provisions made in the solution, not just the technology. Security needs for different applications may be different and dependent on use case. The National Trust Centre (NTC) for M2M services could enhance transparency and security across the ecosystem. In case M2M devices are brought within the trusted framework, it may lead to increased costs and delays and ultimately impact the growth of the M2M sector.

(2) Analysis w.r.t. the Issues Raised Through Q3

2.53 In June 2012, ITU, through the recommendations on 'Overview of the Internet of things' [ITU-T Y.2060 (06/2012)][39] presented a conceptual framework for the IoT. In the recommendation, ITU underscored the importance of security and privacy requirements of IoT. It said, *"through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of "things" to offer services to all kinds of applications, whilst ensuring that <u>security and privacy requirements are fulfilled</u>."* [Emphasis supplied]

2.54 In May 2015, The Government of India released the National Telecom M2M Roadmap[40]. In the roadmap, the Government took specific note of the security and privacy requirements of IoT:

"In the future, M2M/ IoT are likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car and with wearables and ingestible, even the body – poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy."

"For M2M services, in general data security and privacy issues will arise at three levels:

[39] Source: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

[40] Source: https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

(a) M2M data within telecom operator's domain: License conditions enjoin all TSP's to take all necessary steps so as to maintain security of the network & confidentiality of data related to third parties. The encryptions used in the network should conform to the guidelines contained in IT Act. TSPs are limited to providing data transfer mechanism/ media transparently from end devices to M2M platform, hence existing security & encryption related regulation in licenses & IT Act governing current data services should be sufficient to deal with them. The existing provisions of the licenses applicable for TSP's for interception & monitoring of data by the LEAs shall also be applicable in case of M2M services.

(b) M2M data within M2M service provider's domain: M2M will enable creation of wealth of information covering various aspects of economy and society with its potential use for public welfare as well as giving rise to privacy concerns of individuals. The magnified potential for breach of privacy emanate in M2M is due to multiplicity of data recording points in the network i.e. Database of M2M service provider, Data points in database of TSPs, Home Gateways/ devices. The issues require comparison of M2M security and privacy framework with those of existing provisions of IT Act. Also M2M security framework is closely interlinked to interface and architecture standards, on which One M2M alliance and TEC working groups are currently deliberating. Standards need to be followed in conjunction with IT Act, governing current data services, which should be sufficient to deal with such requirements.

(c) Security at sensor/ device level: M2M device should use only genuine IMEIs & ESNs due to security concerns and non-genuine IMEIs & ESNs should not be allowed in devices. Thus, existing IMEIs guidelines for handset will be applicable in case of M2M devices as well.

(d) Security at Network level: M2M will result in availability of large number of devices on Internet or public network and any unauthorized access to/ by these devices may have serious implications. MSPs and TSPs need to device suitable mechanism for their respective network protection."

2.55 In this background, the Authority examined the policy and regulatory initiatives, which have been taken so far, for ensuring security and privacy requirements in IoT domain in India and observed, *inter-alia*, the following developments.

2.56 On 05.09.2017, TRAI issued its recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications'. In these recommendations, TRAI evaluated, *inter-alia*, aspects related to the security of M2M devices. Based on its analysis, TRAI made the following recommendations to DoT through recommendation No. 5.3:

"*a) Device manufacturers should be mandated to implement "Security by design" principle in M2M device manufacturing so that end-to end encryption can be achieved.*

b) The government should provide comprehensive guidelines for manufacturing/ importing of M2M devices in India.

c) A National Trust Centre (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software)."

2.57 On the same day (i.e. on 05.09.2017), DoT issued a gazette notification [GSR 1131(E)][41] on 'Testing and Certification of Telegraph', and mandated, *inter-alia*, the following:

(a) Any telegraph which is used or capable of being used with any telegraph established, maintained, or worked under the license granted by the Central Government in accordance with the provisions of section 4 of the Indian Telegraph Act, 1885 shall have to undergo prior mandatory testing and certification in respect of parameters as determined by the telegraph authority from time to time.

(b) The telegraph authority may by notification in the Official Gazette exempt certain category or categories of telegraph from such mandatory testing.

(c) It shall be the responsibility of the Original Equipment Manufacturer (OEM) in India for getting the mandatory testing and certification done before sale of equipment in India.

(d) It shall be the responsibility of the person importing telegraph for sale in India or the foreign OEM to offer the telegraph for testing and certification by the

[41] Source: https://www.mtcte.tec.gov.in/aboutMTCTE

telegraph authority or its designated body before sale.

(e) Any person licensed or permitted to establish, maintain or work a telegraph under the said Act shall, on detection of use of uncertified telegraph by a user, ensure its removal by the user or, in case of his failure in such removal, withdrawal of service or connectivity to network within seven days of its detection and all such cases shall be brought to the notice of the telegraph authority in each week.

(f) No telegraph in respect of which mandatory certification is required, shall be used by the licenses in its network unless it is certified.

2.58 With respect to the gazette notification on 'Testing and Certification of Telegraph' dated 05.09.2017, Telecom Engineering Center (TEC), in October 2018, issued 'Procedure for Mandatory Testing & Certification of Telecommunication Equipment'[42]. The procedure has been amended from time to time. The salient features of the amended Procedure for Mandatory Testing & Certification of Telecommunication Equipment[43] (MTCTE) issued by TEC are given below:

(a) 'Mandatory Testing & Certification' means testing and certification of Telecom/ related ICT Equipment as per the prescribed procedure.

(b) The scope of certification covers all types of telecom/ related ICT equipment to be sold in India for being used or that may be used for telecommunication. The effective dates for certification becoming mandatory for different products will be notified by the Government separately.

(c) The objective of testing and certification:

(i) that any telecommunication equipment does not degrade performance of the existing network to which it is connected;

(ii) safety of the end users;

(iii) security of telecommunication networks;

(iv) protection of users and general public by ensuring that radio frequency emissions from equipment do not exceed prescribed standards;

[42] Source: https://tec.gov.in/mandatory-testing-and-certification-of-telecom-equipments-mtcte

[43] Source: https://tec.gov.in/pdf/MTCTE/Amend%20MTCTE%20Procedure%20cl%2017%202.pdf

(v) that Telecommunication Equipment complies with the relevant National and International Regulatory Standards and requirements.

(d) Any Original Equipment Manufacturer (OEM)/ Authorised Indian Representative (AIR) who wishes to sell or import any telecom equipment in India, shall have to obtain Certificate from TEC for the notified telecom equipment.

(e) Only complete-in-itself, standalone, independent equipment are tested and certified under MTCTE. Equipment modules/ components are not covered by MTCTE. Further combinations of independent equipment made to form systems are not certified under MTCTE. Instead, each independent equipment should be certified separately.

(f) The equipment needs to be tested in TEC designated Conformity Assessment Bodies (CABs). As a relaxation, test reports/ results from any lab accredited by accreditation bodies under International Laboratory Accreditation Cooperation (ILAC) may be accepted except for those parameters of Essential Requirements (ERs) which are mandatorily to be tested in Indian CABs.

(g) The Essential Requirements (ERs) to be complied for the purpose of certification under MTCTE will include the following:

(i) EMI/ EMC as prescribed by TEC

(ii) Safety as prescribed by TEC

(iii) Technical requirements as prescribed by TEC

(iv) Security requirements as mandated by DoT HQ/ NCCS, Bengaluru from time to time

(v) Other requirements as notified by TEC/ DoT HQ/ any Government agency from time to time.

2.59 In the year 2021, the Government issued the National Security Directive on Telecommunication Sector (NSDTS)[44]. The relevant extract of the NSDTS is given below:

"

1. Telecom is the critical underlying infrastructure for all other sectoral infrastructures of the nation. Security breaches resulting in compromise of the

[44] Source: https://trustedtelecom.gov.in/

confidentiality and integrity of information or in disruption of the infrastructure can have disastrous consequences. Telecom, today, is thus a crucial sector from the National Security perspective.

2. In India, Telecommunication services such as voice, video and data are provided by Telecom Service Providers (TSPs) under licence by the Government, who procure their equipment based on techno-commercial conditions. Recent years have seen a dramatic rise in cyber-attacks, intelligence gathering and influence operations over internet by threat actors. With the increasing use of Internet of Things (loT) devices, the range of possible offensive measures by various actors using telecom network will continue to increase manifold. The advent of 5G technologies will further increase, qualitatively and quantitatively, security concerns resulting from telecom networks.

3. The concerns regarding inimical activities by various state and non-state actors to compromise telecom networks is shared by several other countries. In order to address these concerns, several countries have already taken significant steps, especially with regard to sourcing of telecom products and services. Accordingly, the Government of India has approved the following Directive on 16th December, 2020.

a. Under the provisions of the Directive, in order to maintain the integrity of the supply chain security and in order to discourage insecure equipment in the network, Government will declare a list of Trusted Source/ Trusted Product' for the benefit of the TSPs.

b. The list of equipment to be covered under this Directive and the methodology to designate Trusted Products' will be devised by the Designated Authority who is the National Cyber Security Coordinator (NCSC). TSPs are required to connect new devices which are designated as Trusted Products'.

c. The Designated Authority will make its determination based on approval of a committee headed by Deputy NSA. The committee will consist of members from relevant departments/ Ministries and will also have two members from industry and an independent expert. The Committee will be called 'National Security Committee on Telecom (NSCT)'.

d. The present Directive does not envisage mandatory replacement of the existing equipment already inducted in the networks of the TSPs. The Directive will also not *affect ongoing Annual Maintenance Contracts (AMC) or updates to existing equipment already inducted in the network as on date of effect of the Directive.*

e. From among the sources declared as Trusted Source' by the Designated Authority, those which meet the criteria of Department of Telecom's Preferential Market Access Scheme will be certified as 'Indian Trusted Sources'. The National Security Committee on Telecom will take measures to increase use of equipment from such 'Indian Trusted Sources' in domestic telecom networks.

f. Guidance for the manner in which the 'Enhanced Supervision' and 'Effective Control' could be maintained by TSPs will be issued by Designated Authority at regular intervals. The Department of Telecom will suitably modify its guidelines and ensure monitoring of compliance by TSPs.

g. The Department of Telecom will make appropriate modifications in the license conditions for the implementation of the provisions of the Directive. The policy will come into operation from 15th June, 2021."

2.60 Considering the provisions of the NSDTS, DoT has made the following amendment in the Unified License Agreement:

"39.7.1. The Government through the Designated Authority will have the right to impose conditions for procurement of Telecommunication Equipment on grounds of Defence of India, or matters directly or indirectly related thereto, for national security. Designated Authority for this purpose shall be National Cyber Security Coordinator. In this regard, the licensee shall provide any information as and when sought by the Designated Authority.

Designated Authority shall notify the categories of equipment for which the security requirement related to Trusted Sources are applicable. For the said categories of equipment, Designated Authority shall notify the Trusted Sources along with the associated Telecommunication Equipment (Trusted Products). The Designated Authority may also notify a list of Designated Sources from whom no procurement can be done. Procedure for inclusion of Telecommunication Equipment in the list of Trusted Sources will be issued by the Designated Authority.

With effect from 15th June 2021, the licensee, shall only connect Trusted Products in its network and also seek permission from Designated Authority for upgradation *or expansion of existing Network utilizing the Telecommunication Equipment not designated as Trusted Products. However, these directions will not affect ongoing Annual Maintenance Contracts (AMC) or updates to existing equipment already inducted in the network as on date of effect.*

The licensees shall comply with the Guidance for Enhanced Supervision and Effective Control of Telecommunication Networks, as per guidelines to be issued by the licensor."

2.61 With respect to recommendation No. 5.3(c) of the Recommendations dated 05.09.2017 [as mentioned in para 2.56 above], Telecom Engineering Center (TEC), in March 2022, issued a technical report (TEC 31188:2022)[45] on 'Framework of National Trust Centre for M2M/ IoT Devices and Applications'. The salient points of the technical report are given below:

(a) Prior to their sale/ deployment in India, all IoT/ M2M devices should be got tested by the manufacturer as per MTCTE Essential Requirements (hardware testing) and by STQC (Software testing).

(b) The Government should establish a National Trust Centre (NTC). NTC should have repository of certified IoT/ M2M devices as well as the related manufacturers from MTCTE portal and the uncertified devices (already deployed/ not covered in MTCTE).

(c) If M2M/ IoT devices are hacked or become vulnerable, it should be detected by IoT platforms and intimated to NTC.

(d) The repository of NTC should also have the record of vulnerabilities as discovered in M2M/ IoT devices to provide a mechanism of continuous improvement in safety and security of the devices and the networks.

2.62 In the technical report (TEC 31188:2022), TEC also included a conceptual diagram of the National Trust Center, as given below:

[45] Source: https://tec.gov.in/pdf/M2M/TR_National%20Trust%20Center_TEC%2031188_2022.pdf

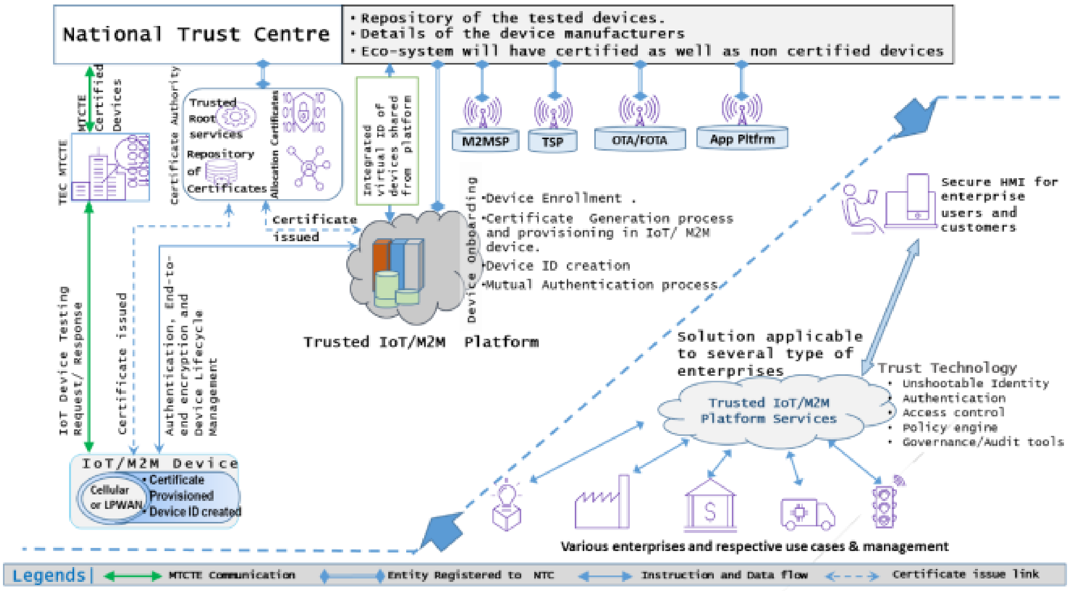

National Trust Centre
• Repository of the tested devices.
• Details of the device manufacturers
• Eco-system will have certified as well as non certified devices
MTCTE Certified Devices
TEC MTCTE
Certificate Authority
Trusted Root services
Repository of Certificates
Allocation Certificates
Integrated virtual ID of devices shared from platform
M2MSP
TSP
OTA/FOTA
App Pltfrm
Certificate issued
Device Onboarding
•Device Enrollment .
•Certificate Generation process and provisioning in IoT/ M2M device.
•Device ID creation
•Mutual Authentication process
Trusted IoT/M2M Platform
IoT Device Testing Request/ Response
Certificate issued
Authentication, End-to-end encryption and Device Lifecycle Management
IoT/M2M Device
Cellular or LPWAN
• Certificate Provisioned
• Device ID created
Secure HMI for enterprise users and customers
Solution applicable to several type of enterprises
Trusted IoT/M2M Platform Services
Trust Technology
• Unshootable Identity
• Authentication
• Access control
• Policy engine
• Governance/Audit tools
Various enterprises and respective use cases & management
Legends
MTCTE Communication
Entity Registered to NTC
Instruction and Data flow
Certificate issue link

Figure 2.3: TEC's conceptual diagram of the National Trust Center[46]

2.63 In December 2023, the Indian Parliament enacted the Telecommunications Act, 2023[47]. Section 3 of the Act provides as below:

"3. (1) Any person intending to—

(a) provide telecommunication services;

(b) establish, operate, maintain or expand telecommunication network; or

(c) possess radio equipment,

shall obtain an authorisation from the Central Government, subject to such terms and conditions, including fees or charges, as may be prescribed."

2.64 Based on a reference from DoT, the Authority, on 18.09.2024, has sent its recommendations on 'the Framework for Service Authorisations to be Granted Under the Telecommunications Act, 2023'. Through these recommendations, the Authority has recommended, *inter-alia*, that M2M Service and WLAN/ WPAN Connectivity Service Providers should be authorised under section 3(1)(a) of the Telecommunications Act, 2023. The entities authorised under the Telecommunications Act, 2023 will have to adhere to various rules made under the Act including the rules on standards and security made under Section 19 and Section

[46] Source: https://tec.gov.in/pdf/M2M/TR_National%20Trust%20Center_TEC%2031188_2022.pdf

[47] Source: https://egazette.gov.in/WriteReadData/2023/250880.pdf

21 of the Act. Relevant extracts of Section 19 and Section 21 of the Act are reproduced below:

"19. The Central Government may notify standards and conformity assessment measures in respect of—

(a) telecommunication equipment, telecommunication identifiers and telecommunication network;

(b) telecommunication services, in consonance with any regulations notified by the Telecom Regulatory Authority of India from time to time;

(c) manufacture, import, distribution and sale of telecommunication equipment;

(d) telecommunication security, including identification, analysis and prevention of intrusion in telecommunication services and telecommunication networks;

(e) cyber security for telecommunication services and telecommunication networks; and

(f) encryption and data processing in telecommunication.

"21. The Central Government may, if satisfied that it is necessary or expedient so to do, in the interest of national security, friendly relations with foreign States, or in the event of war, by notification take such measures as are necessary in the circumstances of the case, including issuing directions in respect of the following, namely:-

...

(d) procurement of telecommunication equipment and telecommunication services only from trusted sources;" (Emphasis supplied)

2.65 The Authority is of the view that owing to the pervasive nature of the deployment of IoT devices in all walks of life, the importance of security and privacy requirements of IoT cannot be over-emphasized. In this regard, the Authority notes that the Government has already laid down the following frameworks for ensuring security of telecommunication ecosystem:

(a) NSDTS: Trusted Source/ Trusted Product framework - applicable on all licensed/ authorised telecom service providers (TSPs) – to maintain integrity of the supply chain security and to discourage insecure equipment in the telecommunication networks

(b) MTCTE: Framework for mandatory testing and certification of telecom equipment – applicable on all original equipment manufacturers (OEMs) – to ensure, *inter-alia*, the security of telecommunication networks.

2.66 Apart from the above, the Government, based on the TRAI's recommendations dated 05.09.2017, is also considering the implementation of National Trust Center (NTC). The proposed NTC will comprise a repository of certified IoT/ M2M devices, and a record of vulnerabilities as discovered in the IoT/ M2M devices. In essence, the proposed NTC will provide a mechanism for the continuous improvement in safety and security of IoT devices and networks.

2.67 The Authority is of the view that the trinity of NSDTS, MTCTE, and NTC, once fully implemented in respect of IoT/ M2M, will provide a comprehensive framework for ensuring a secure IoT ecosystem.

2.68 In this regard, the Authority perused the list of telecom products notified under MTCTE[48]. As per the list notified by TEC on its website, 211 telecom products have been notified under MTCTE till date, out of which, only the following six telecom products belong to the IoT/ M2M domain:

(a) IoT Gateway

(b) Asset tracking device

(c) Human tracking device

(d) Pet tracking device

(e) Standalone tracking device for vehicle

(f) Smart electricity meter

2.69 With the passage of time, a plethora of devices have begun to be used in IoT/ M2M domain. An illustrative list of IoT products is given below:

[48] Source: https://www.mtcte.tec.gov.in/filedownload?name=downloadDocument_ProductsList.docx

S. No.	IoT Category	Product category	Product
1	Consumer IoT	Smart Home Devices	Smart speakers
2			Smart TVs
3			Smart thermostats
4			Smart lighting
5			Smart locks
6			Smart security systems (cameras, alarms)
7			Smart appliances (refrigerators, ovens)
8		Wearables	Smartwatches
9			Fitness trackers
10			Health monitoring devices
11		Other Consumer Devices	Smart toys
12			Autonomous vehicles
13	Industrial IoT	Sensors	Temperature sensors
14			Pressure sensors
15			Motion sensors
16			Chemical sensors
17			Image sensors
18			Air quality sensors
19			Biomedical sensors
20		Industrial Machinery & Equipment	Manufacturing machinery
21			Robotics
22			Asset tracking devices
23		Infrastructure	Smart grids
			Smart metering systems
24			Smart transportation systems
25			Environmental monitoring systems
26	Commercial IoT	Healthcare	Remote patient monitoring
27			Wearable medical devices

S. No.	IoT Category	Product category	Product
28			Medical imaging devices
29		Retail	Point-of-sale (PoS) systems
30			Inventory management systems
31			Customer analytics
32		Logistics	GPS trackers
33			Fleet management systems
34		Agriculture	Smart farming technologies
35			Precision irrigation systems
36			Crop monitoring systems
37		Security	Security cameras
38			Access control systems
39			Surveillance systems

Table 2.1: Illustrative list of IoT products

2.70 Generally, IoT products are deployed in insecure or physically exposed environments. Besides, at the manufacturer's level, there is limited security planning and weak architecture for operating system, application including development methodologies[49]. Therefore, IoT devices, services and software, and the communication channels that connect them, are at risk of attack by a variety of malicious parties, from casual hackers to professional criminals or even state actors[50]. In short, there is a significant security risk in respect of IoT devices.

2.71 The Authority notes that the National Critical Information Infrastructure Protection Centre (NCIIPC)[51], which is the national nodal agency in respect of Critical Information Infrastructure Protection in India, has identified Power & Energy, Banking, Financial Services & Insurance, Telecommunication, Transport,

[49] Source: https://tec.gov.in/public/pdf/M2M/Security%20by%20Design%20for%20IoT%20Device%20Manufacturers.pdf

[50] Source: https://tec.gov.in/pdf/M2M/TR_National%20Trust%20Center_TEC%2031188_2022.pdf

[51] NCIIPC, a unit of NTRO, is an organisation of the Government of India created under Sec 70A of the Information Technology Act, 2000. Source: https://nciipc.gov.in/about_us.html

Government, Strategic & Public Enterprises, and Healthcare as critical sectors[52]. As per NCIIPC, there are severe threats that may cause systemic harm to entities and organisations in 'critical sectors' of the nation, further impacting national security, economy, public health and safety[53].

2.72 The Authority is cognizant of the fact that security and privacy concerns from IoT devices emanate essentially from the M2M communication modules embedded in them through which IoT devices get connected to telecommunication networks including public internet. Accordingly, the Authority is of the view that to allay security and privacy concerns in respect of IoT devices, particularly those which are used in critical sectors, the M2M communication modules embedded/ plugged in IoT devices (which are capable of being connected to telecommunication networks) require to be notified under MTCTE.

2.73 Considering the foregoing discussion, **the Authority recommends that the M2M communication modules embedded/ plugged in all IoT devices (which are capable of being connected to telecommunication networks) deployed in the critical sectors identified by National Critical Information Infrastructure Protection Centre (NCIIPC), Government of India should be notified under the framework of Mandatory Testing & Certification of Telecommunication Equipment (MTCTE) in a phased manner. IoT devices deployed in the remaining sectors may be notified under MTCTE at a subsequent stage.**

2.74 On the aspect of bringing M2M devices under the Trusted Source/ Trusted Product framework, the Authority took note of the following aspects:

(a) In the year 2021, the Government amended the Unified License and included a provision that "*Designated Authority shall notify the categories of equipment for which the security requirement related to Trusted Sources are applicable. For the said categories of equipment, Designated Authority shall notify the*

[52] Source: https://nciipc.gov.in/documents/CAF/Book_Supplementary-Technical-Criteria_Level-2_v.P_31.03.2024.pdf

[53] ibid

Trusted Sources along with the associated Telecommunication Equipment (Trusted Products). …With effect from 15th June 2021, the licensee, shall only connect Trusted Products in its network…"

(b) Section 21(d) of the Telecommunication Act, 2023 provides that the Central Government may, if satisfied that it is necessary or expedient so to do in the interest of national security, friendly relations with foreign States, or in the event of war, take necessary measures including issuing directions in respect of the procurement of telecommunication equipment and telecommunication services only from trusted sources.

2.75 As the matter relates to national security, friendly relations with foreign States etc., the Authority is of the view that it should be left to the Government to decide the category of equipment in respect of which the security requirements related to Trusted Sources should apply.

D. Transfer of Ownership of M2M SIMs

2.76 Subscriber Identity Modules (SIMs) are used for providing telecommunication services using 3GPP[54] standards. A subscriber obtains a SIM from its access service provider when a new cellular mobile connection is activated in his name. SIMs contain communication profiles that uniquely identify cellular mobile subscriptions. A communications profile includes Mobile Station International Subscriber Directory Number (MSISDN) and International Mobile Subscriber Identity (IMSI). Generally, the SIMs, which are used for Person-to-Person (P2P) mobile communication, are referred to as consumer SIMs. On the other hand, the SIMs, which are used for Machine-to-Machine (M2M) mobile communication, are referred to as M2M SIMs.

2.77 As per the extant licensing framework in the country, the change in the name of subscriber, in the case of consumer mobile connections, is permitted only between

[54] Source: https://www.3gpp.org/

blood relatives/ legal heirs. The relevant extract of the DoT's instructions dated 09.08.2012[55] in this regard is reproduced below:

"*7. Change in the name of subscriber*

(i) The change of name of subscriber is not permitted as the SIM card in user terminal is not transferable. The change in name between the blood relatives/ legal heirs is permitted provided new CAF and all the procedure as for registering a new subscriber is followed and new SIM Card is issued. However, after the change in name the connection shall be treated as new connection. In such case, change in address is not permitted. Further, No Objection Certificate from the original user shall also be taken. In case of death of the original user, death certificate will suffice instead of No Objection Certificate."

2.78 As per the DoT's instructions[56] on the issuance of M2M SIMs dated 16.05.2018 read with the DoT's Guidelines[57] for Registration Process of M2M Service Providers (M2MSP) & WPAN/ WLAN Connectivity Provider for M2M Services dated 08.02.2022 (hereinafter, referred to as, "the M2MSP Guidelines"), an access service provider may grant M2M mobile connections to M2MSP registrants only. As per the M2MSP Guidelines, the M2MSP registrants are authorized to *"provides M2M services to third parties using telecom resources. Provided that (a) such third parties utilising M2M services from registered M2MSP in connection with its products or as part of its offerings to its end customers as a product or service, and (b) any organization which intends to provide M2M services for its own use (captive use) and not for commercial purpose, shall also be covered under this definition."*[58]

2.79 The M2MSP Guidelines also provides that *"[t]he details of all the customers of M2M services i.e., physical custodian of machines fitted with SIMs, shall be maintained by M2MSP. Up-dated information regarding (a) details of M2M end device i.e. IMEI,*

[55] Source: https://dot.gov.in/sites/default/files/Instructions%20on%20Verification%20of%20New%20Mobile%20Subscribers%20%281%29.PDF?download=1

[56] Source: https://dot.gov.in/sites/default/files/M2M%20Guidelines.PDF?download=1

[57] Source: https://dot.gov.in/sites/default/files/M2MSP%20Guidelines%20.pdf?download=1

[58] Source: https://dot.gov.in/sites/default/files/M2MSP%20Guidelines%20.pdf?download=1

ESN etc., (b) Make, Model, Registration number etc. of the machines (i.e. Cars, Utility Meters, POS etc.) & (c) corresponding physical custodian's name and address shall be made available to Authorized Telecom Licensee and designated Authority by M2MSP. Any changes in customers and machines details shall be updated."

2.80 While the change in the name of end customers of M2M services (custodians of the machines fitted with M2M SIMs) is permitted under the extant M2MSP Guidelines, there is no provision for the change in the name of the owner of M2M SIMs i.e. M2MSPs.

2.81 In this background, DoT, through the Reference dated 01.01.2024, has conveyed to TRAI that the industry has requested to allow the transfer of ownership of M2M SIMs, and requested TRAI to provide its recommendations on the transfer of ownership of M2M SIMs.

2.82 In this context, the Authority, through the Consultation Paper dated 24.06.2024, solicited comments from stakeholders on the following question:

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 the new M2MSP for providing connectivity to the existing customers?

Please provide a detailed response with justifications.

(1) Responses of Stakeholders on Q4

2.83 In response to Q4, most stakeholders have suggested that there is a need to establish a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs. However, a couple of stakeholders have contended against it.

2.84 A summary of the comments from the stakeholders, who have suggested that there is a need to establish a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs, is given below:

(a) In many cases, either M2MSP stops its services due to financial constraints or for some other reason or gets acquired by another entity. In such cases, existing customers have no choice except to close the service or discard the device and buy a new device. To avoid such situations, a framework for the change of ownership of SIMs amongst M2MSPs must be established.

(b) There is a need to establish a regulatory framework for the transfer of ownership of M2M SIMs amongst M2MSPs to avoid service disruptions and inconvenience to users, and to ensure a seamless, secure, and efficient transition.

2.85 A stakeholder, who has contended that there is no need for establishing a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs, has stated that the M2M/ IoT sector is at a nascent stage in India; such a regulatory framework should be introduced only when the M2M market gets matured enough.

2.86 A broad summary of the comments from the stakeholders in response to Q4(a) with respect to salient features of the regulatory framework for the transfer of the ownership of M2M SIMs among M2MSPs is given below:

(a) As M2M SIMs are used for various critical services, and embedded M2M SIMs are being used exceedingly in this sector, there is a need for explicit guidelines for an efficient transfer of ownership of M2M SIMs.

(b) The process of the transfer of the ownership of M2M SIMs should be customer-centric and ensure seamless service to the end-user. Any sort of service disruption or any explicit action from end-user should be avoided at all costs.

(c) All terms and conditions pertaining to the transfer of M2M SIMs should be mutually agreed upon, including the service level agreements (SLAs) and *inter-se* 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 and there should be no regulatory intervention.

(d) The new entity must meet subscriber verification norms (KYC verification) and maintain updated records.

(e) There should be a requirement of obtaining No Objection Certificates (NOCs) for the transfer of ownership from both outgoing and new entities; in cases where the outgoing entity ceases to exist, then the new entity should categorically declare the same. The format of the NOC may be suggested by DoT.

(f) Since physical M2M SIMs are installed in extended geographies, there should be no requirement of the issuance of new M2M SIMs or deactivation/ reactivation of M2M SIMs. The transferred M2M 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.

(g) The new M2MSP must give an undertaking to take over all the responsibilities of M2MSP.

(h) The features for the transfer of ownership of M2M SIMs among M2MSPs should be like the conditions mentioned for licensed telecom service providers.

2.87 A broad summary of the comments from the stakeholders in response to Q4(b) with respect to scenarios in which the transfer of the ownership of M2M SIMs should be permitted is given below:

(a) In case of merger, demerger, or acquisition of the existing M2MSP

(b) For cases involving the transfer of ownership from the parent company to its subsidiary/ other group company or *vice-versa,* and between its subsidiaries/ group companies

(c) For cases where the enterprise customer seeks to change the existing M2MSP and opt for a new M2MSP for better service, pricing, or other reasons

(d) In case of business closure or bankruptcy of M2MSP

2.88 A summary of comments from stakeholders in response to Q4(c) with respect to measures to be taken to avoid any misuse of the facility for the transfer of the ownership of M2M SIMs is given below:

(a) To avoid any misuse, KYC rules must be followed for the new entity in whose name the M2M SIMs are to be transferred.

(b) Prior to the transfer of M2M SIMS from one M2MSP to another, the details of the transferee M2MSP, along with a No Objection Certificate (NOC) conveying concurrence of both the transferor and the transferee should be provided to the licensed access service provider(s) by the transferor M2MSP.

2.89 A summary of the comments from the stakeholders in response to Q4(d) with respect to the flexibility to be given to a new M2MSP for providing connectivity to the existing customers is given below:

(a) The transfer of ownership should not require any explicit action from end users.

(b) There should be no need to record the data pertaining to the transfer of ownership on Saral Sanchar portal.

(2) Analysis w.r.t. the Issues Raised Through Q4

2.90 As per the DoT's instructions dated 16.05.2018[59], "*for M2M services, the mobile connections shall be issued by the licensees in the name of entity/ organization providing M2M Services ....*" Meaning thereby, M2MSPs own the M2M SIMs.

2.91 As per the extant licensing framework in the country, the change in the name of subscriber of consumer mobile connections is permitted between blood relatives/ legal heirs; however, there is no provision for the change in the name of the owner of M2M SIMs.

2.92 As per the M2MSP Guidelines[60], in case of merger or acquisition of an M2MSP, "*the registration granted cease to exist and the new entity has to re-register.*" As the M2MSP registration does not get transferred upon merger or acquisition under the extant regime, upon merger or acquisition of an existing M2MSP (acquired entity),

[59] Source: https://dot.gov.in/sites/default/files/M2M%20Guidelines.PDF?download=1

[60] Source: https://dot.gov.in/sites/default/files/M2MSP%20Guidelines%20.pdf?download=1

M2M SIMs held by the M2MSP do not get transferred to the resultant entity (acquiring entity) automatically. The resumption of the M2M business would require the following steps to be taken:

(a) The Access Service Provider deactivates the M2M SIMs given to the acquired entity, as it no longer holds M2MSP registration.

(b) Meanwhile, the resultant entity obtains M2MSP registration from DoT.

(c) The new M2MSP registration holder (resultant entity) requests the Access Service Provider to grant the same M2M SIMs to it.

(d) The Access Service Provider reactivates the M2M SIMs in the name of the resultant entity.

2.93 Clearly, such a process would require deactivation/ reactivation of M2M SIMs which may entail disruption of M2M service to end customers and thereby result in consumer inconvenience and loss of business.

2.94 As there is no provision for the change in the name of the owner of M2M SIMs under the extant regime, M2M services for the affected end consumers may get disrupted whenever there is a situation requiring the change of M2MSP. Such a situation may arise in numerous scenarios, including the following:

(a) In case of merger, demerger, or acquisition of the existing M2MSP

(b) For cases involving the transfer of M2MSP business from the parent company to its subsidiary/ other group company or *vice-versa,* and between its subsidiaries/ group companies

(c) In case the enterprise customer seeks to change the existing M2MSP and opts for a new M2MSP for better service, pricing, or other reasons

(d) In case of business closure or bankruptcy of M2MSP

2.95 The Authority is of the view that the possibility of M2M service disruption in the afore-mentioned scenarios may be avoided by introducing the following regulatory provisions:

(a) In matters related to merger, demerger, acquisition etc.: There is a need to introduce an enabling policy framework for the transfer of M2MSP registration/

authorisation to the resultant entity in case of merger, demerger, acquisition etc. of M2MSP entities. This policy framework should be analogous to the policy framework for the transfer of Unified License. Specifically, all M2M SIMs held by the acquired entity (under the M2MSP registration/ authorisation[61]) should automatically be transferred to the resultant entity.

(b) <u>In the remaining cases</u>: There is a need to introduce an enabling provision for the transfer of ownership of M2M SIMs from one M2MSP to another if the transferor entity furnishes a no objection certificate (NOC) for such a transfer and the transferee company furnishes an undertaking for taking over all responsibilities of M2M SIMs, to the service access service provider(s).

2.96 With respect to the scenario mentioned in para 2.95 (a), the following aspects are worth noting:

(a) The extant licensing regime under the Indian Telegraph Act, 1885 permits the transfer of telecommunication service licenses/ authorisations. In this regard, DoT has already devised 'Guidelines for Transfer/ Merger of various categories of Telecommunication service licences/ authorisation under Unified Licence (UL) on compromises, arrangements and amalgamation of the companies' dated 20.02.2014.

(b) Section 3(5) of the Telecommunications Act, 2023 provides that "*[a]ny authorised entity may undertake any merger, demerger or acquisition, or other forms of restructuring, subject to any law for the time being in force and any authorised entity that emerges pursuant to such process, shall comply with the terms and conditions, including fees and charges, applicable to the original authorised entity, and such other terms and conditions, as may be prescribed.*" In this context, the Authority, through its recommendations on 'the Framework for Service Authorisations to be Granted Under the Telecommunications Act, 2023' has included a provision on the transfer of M2M Service and WLAN/

[61] The Authority, through its recommendations on 'the Framework for Service Authorisations to be Granted Under the Telecommunications Act, 2023' dated 18.09.2024 has recommended that *"[t]he Unified Service Authorised Entity, Access Service Authorised Entity and M21M WAN Service Authorised Entity can provide M2M Service …"* In this regard, para 4(5) on page 721 of the recommendations dated 18.09.2024 may kindly be referred to.

WPAN Connectivity Service Authorisation. In this regard, para 5(3) on page 722 of the recommendations dated 18.09.2024 may kindly be referred to.

2.97 Considering the foregoing discussion, **the Authority recommends that-**

(a) DoT should establish a framework for the transfer of M2M Service Provider (M2MSP) registration/ authorisation to the resultant entity in case of merger, demerger, acquisition etc. of M2MSP entities.

(b) DoT should introduce an enabling provision for the transfer of the ownership of M2M SIMs from one M2MSP registration holder/ authorised entity to another if –

(i) The transferor entity furnishes a no objection certificate (NOC) for the transfer of M2M SIMs, and

(ii) The transferee entity furnishes an undertaking for taking over all responsibilities of M2M SIMs (obtained from the transferor entity) to the access service provider(s) concerned.

(c) Upon transfer of M2M SIMs, the access service provider(s) concerned should promptly amend the name of the owner of M2M SIMs in its subscriber database.

2.98 The Authority also noted that many stakeholders have emphasized the need for mandating the transferee M2MSP entity to maintain updated records in respect of M2M SIMs obtained from the transferor company. In this regard, the Authority took cognizance of the following provisions of the DoT's instructions[62] on the issuance of M2M SIMs dated 16.05.2018:

"6. … The details of all the customers of M2M services i.e., physical custodian of machines fitted with SIMs should be maintained by entity/ organization providing M2M Services. Updated information regarding (a) Details of M2M end device i.e. IMEI/ ESN etc. (b) Make Model Registration no. etc. of the machines (i.e. Cars Utility Meters POS etc.) and (c) Corresponding physical custodian's name and address should be made available online through some web interface to Licensee by entity/organization providing M2M Services. Regarding maintenance of

[62] Source: https://dot.gov.in/sites/default/files/M2M%20Guidelines.PDF?download=1

database/records of the end users of the SIM cards by the Licensee, the procedure as prescribed for bulk connection shall be followed.
7. In case of sale or transfer of devices having M2M SIMs inside it the responsibility of intimating to the Licensees the details of person to whom such devices are transferred and for fulfilling subscriber verification norms lies with the entity/organization providing M2M Services i.e. the entity/organization which has taken such SIMs from the licensee. The Licensees shall regularly update all these details in their database."

2.99 A similar provision is also contained in para 4 of Chapter III of the M2MSP Guidelines[63] as well.

2.100 Considering the above, **the Authority recommends that the transferee M2MSP entity should maintain the updated details of physical custodians of machines fitted with M2M SIMs obtained from the transferor entity and provide the same to the concerned access service provider(s).**

E. Miscellaneous Issues

2.101 Through the Consultation Paper dated 24.06.2024, the Authority solicited comments from stakeholders on the following question:
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.

2.102 A broad summary of comments from stakeholders in response to Q5 is given below:

(a) TRAI should review its recommendation that all communication profiles on any M2M eSIM fitted in an imported device on international roaming in India should be mandatorily converted/ reconfigured into communication profiles of Indian

[63] Source: https://dot.gov.in/sites/default/files/M2MSP%20Guidelines%20.pdf?download=1

telecom service providers within a period of six months from the date of activation of international roaming in India.

(b) GSMA standards for SM-SR and SM-DP should be followed in India. M2MSPs should be allowed to have their own SM-SR and SM-DP subject to conformance of GSMA standards.

(c) ITU allocated series 901.XX (Global IMSI) should be allowed to be used in India.

(d) Service providers using RF mesh technology should be brought under the ambit of M2M authorisation of Unified License.

(e) No additional frequency spectrum should be delicensed for the purpose of providing M2M service.

2.103 The Authority perused the comments from stakeholders on Q5. The Authority observed that the stakeholders' suggestions (a), (b) and (c), mentioned in para 2.102 above, contain aspects on which the Authority has recently made recommendations through the 'Recommendations on Usage of Embedded SIM for Machine-to-Machine (M2M) Communications' dated 21.03.2024 after a comprehensive consultation with stakeholders. The suggestions (d) and (e) made by stakeholders are beyond the scope of the present consultation. TRAI will examine such aspects in case the need arises, and DoT sends a reference to TRAI to make recommendations on them.

2.104 The following chapter provides a summary of recommendations.

CHAPTER III

SUMMARY OF RECOMMENDATIONS

3.1 **Earlier, through the recommendation No 5.1 (g) of the recommendations on Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017, TRAI 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".* Based on a review of this recommendation, the Authority recommends as below:**

(a) A service (application) should be classified as a 'critical IoT service' if it passes the following twin tests:

(i) Whether the service (application) demands ultra-reliable low-latency M2M connectivity with very high availability?

(ii) Whether any disruption of the M2M connectivity used for delivering the service (application) will have a debilitating impact on national security, economy, public health, or public safety?

(b) Instead of classifying an entire domain/ sector as a critical IoT sector, specific IoT services (applications) within the domain/ sector should be classified as critical IoT services.

(c) The classification of critical IoT services of a particular domain/ sector should be done by the ministry/ regulatory body concerned in consultation with DoT.

(d) Any IoT service should be treated as a non-critical IoT service unless it is identified and notified as a critical IoT service.

(e) For the classification of critical IoT services, DoT should devise an institutional mechanism for the assistance of concerned ministries/ regulatory bodies. The institutional mechanism may include the following aspects:

(i) The classification of critical IoT services of each domain/ sector

should be done on the basis of the recommendations of a standing committee comprising of one or more officers nominated by the ministry/ regulatory body concerned and an officer nominated by DoT. The standing committees should also recommend service performance benchmarks (such as latency, reliability, availability etc.) for each critical IoT service.

(ii) After considering the standing committee's recommendations, the concerned ministry/ regulatory body should notify the regulatory requirements including the telecommunication service performance benchmarks (such as latency, reliability, availability etc.) for each critical IoT service separately.

(iii) DoT, as the nodal department, should establish an online repository of sector-wise critical IoT services and corresponding regulatory requirements including telecommunication service performance benchmarks, as prescribed by the concerned ministries/ regulatory bodies. The online repository should be accessible to the general public.

(f) Any wireless M2M communication technology (utilizing unlicensed spectrum, or licensed spectrum) or wired M2M communication technology should be permitted to be used for the provision of critical IoT services if it meets the prescribed service performance benchmarks. The choice for M2M communication technologies may be exercised by user agencies based on their techno-commercial considerations.

[Para 2.45]

3.2 **The Authority recommends that the M2M communication modules embedded/ plugged in all IoT devices (which are capable of being connected to telecommunication networks) deployed in the critical sectors identified by National Critical Information Infrastructure Protection Centre (NCIIPC), Government of India should be notified under the framework of Mandatory Testing & Certification of Telecommunication**

Equipment (MTCTE) in a phased manner. IoT devices deployed in the remaining sectors may be notified under MTCTE at a subsequent stage.

[Para 2.73]

3.3 **The Authority recommends that-**

(a) DoT should establish a framework for the transfer of M2M Service Provider (M2MSP) registration/ authorisation to the resultant entity in case of merger, demerger, acquisition etc. of M2MSP entities.

(b) DoT should introduce an enabling provision for the transfer of the ownership of M2M SIMs from one M2MSP registration holder/ authorised entity to another if –

(i) The transferor entity furnishes a no objection certificate (NOC) for the transfer of M2M SIMs, and

(ii) The transferee entity furnishes an undertaking for taking over all responsibilities of M2M SIMs (obtained from the transferor entity) to the access service provider(s) concerned.

(c) Upon transfer of M2M SIMs, the access service provider(s) concerned should promptly amend the name of the owner of M2M SIMs in its subscriber database.

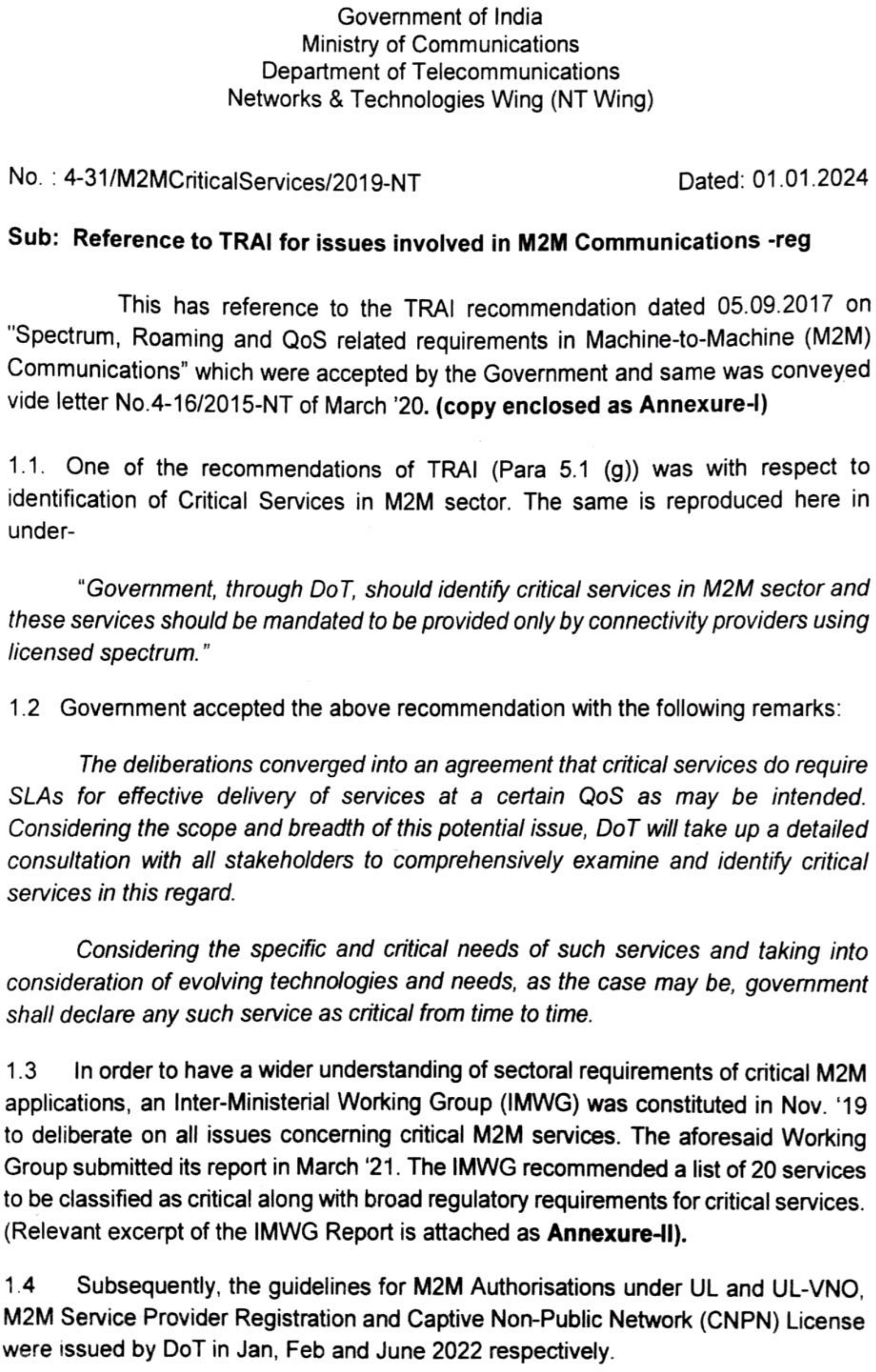
[Para 2.97]

3.4 **The Authority recommends that the transferee M2MSP entity should maintain the updated details of physical custodians of machines fitted with M2M SIMs obtained from the transferor entity and provide the same to the concerned access service provider(s).**

[Para 2.100]

ANNEXURE I

DoT's Reference Dated 01.01.2024



Government of India
Ministry of Communications
Department of Telecommunications
Networks & Technologies Wing (NT Wing)

No. : 4-31/M2MCriticalServices/2019-NT Dated: 01.01.2024

Sub: Reference to TRAI for issues involved in M2M Communications -reg

This has reference to the TRAI recommendation dated 05.09.2017 on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" which were accepted by the Government and same was conveyed vide letter No.4-16/2015-NT of March '20. **(copy enclosed as Annexure-I)**

1.1. One of the recommendations of TRAI (Para 5.1 (g)) was with respect to identification of Critical Services in M2M sector. The same is reproduced here in under-

"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."

1.2 Government accepted the above recommendation with the following remarks:

The deliberations converged into an agreement that critical services do require SLAs for effective delivery of services at a certain QoS as may be intended. Considering the scope and breadth of this potential issue, DoT will take up a detailed consultation with all stakeholders to comprehensively examine and identify critical services in this regard.

Considering the specific and critical needs of such services and taking into consideration of evolving technologies and needs, as the case may be, government shall declare any such service as critical from time to time.

1.3 In order to have a wider understanding of sectoral requirements of critical M2M applications, an Inter-Ministerial Working Group (IMWG) was constituted in Nov. '19 to deliberate on all issues concerning critical M2M services. The aforesaid Working Group submitted its report in March '21. The IMWG recommended a list of 20 services to be classified as critical along with broad regulatory requirements for critical services. (Relevant excerpt of the IMWG Report is attached as **Annexure-II).**

1.4 Subsequently, the guidelines for M2M Authorisations under UL and UL-VNO, M2M Service Provider Registration and Captive Non-Public Network (CNPN) License were issued by DoT in Jan, Feb and June 2022 respectively.

1.5 Considering the introduction of aforesaid new license (UL-M2M) and registration policy, comments were solicited from all relevant stakeholders in the M2M/IoT ecosystem (including key line ministries, registered M2M Service Providers and other stakeholders) on the IMWG Report and SLA required for Critical Services. The list of stakeholders who have provided comments, is placed at **Annexure-III.**

2. Following points have emerged based on the comments received from various stakeholders necessitating a need to revisit and examine afresh the abovesaid recommendation-

I. **Use of licensed spectrum may not be made mandatory for critical services/sector, if the requisite Service Level Agreements (SLAs)/Quality of Service (QoS) can be met through unlicensed spectrum.** Many Start-ups/companies are designing their model to operate in license-free band. 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. Further, the relationship between security of M2M services and these services operating on licensed spectrum was not cogent.

II. 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.** Further, the SLA/QoS framework along-with detailed regulatory requirement for the same may also be defined by respective concerned ministries/regulatory bodies for different use cases (which are identified as critical) and implementing technologies may comply with the same.

III. **A balanced approach of utilizing both licensed and unlicensed bands may be the way forward to improve customer experience, drive innovation and increase affordability.** Connectivity may be left to the discretion of the customer/ministries based on service parameters required for an application and not be enforced.

IV. Critical M2M services may require robust, resilient, reliable, redundant and secure network. However, with the ever-growing interconnectivity of devices in the Internet of Things (IoT) and Machine-to-Machine (M2M) domains, it has now become crucial to ensure the security and trustworthiness of these devices. Therefore, bringing M2M/IoT devices under the Trusted Source-Trusted Product regulation, specifically mandating the procurement of M2M/IoT devices for Critical Infrastructure Sectors, as defined in the National Critical Information Infrastructure Protection Centre (NCIIPC) regulations can significantly mitigate the threat landscape and enhance the security posture of critical infrastructure sectors *rather than merely mandating provision of these services by connectivity providers using licensed spectrum.*

3. Secondly, as per extant instructions, SIMs are non-transferable. A provision was introduced vide DoT instructions dated 16.05.18 to update the details of person to whom device is transferred in the database of the licensee (as intimated by M2M SP to the licensee) in case the devices with M2M SIM(s) are sold or transferred, However, there is no provision for change in the name of the owner of the M2M SIM.

3.1 Industry has requested to allow the transfer of ownership of M2M SIMs for the following scenarios:

i. Involving mergers, acquisitions, takeover of companies.

ii. For cases where 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.

iii. For cases where M2MSP is ceasing its operations or is filing for bankruptcy, etc. and the M2M SIMs are required to be either transferred to the new M2MSP or directly to the company where M2M SIMs are used/deployed.

3.2 It is therefore necessary to examine the issue related to Transfer of ownership in case of M2M SIMs in view of situations narrated at 3.1 above.

4. Accordingly, TRAI is requested to provide reconsidered recommendations, as per provisions of Section 11 of the TRAI Act 1997 as amended from time to time on

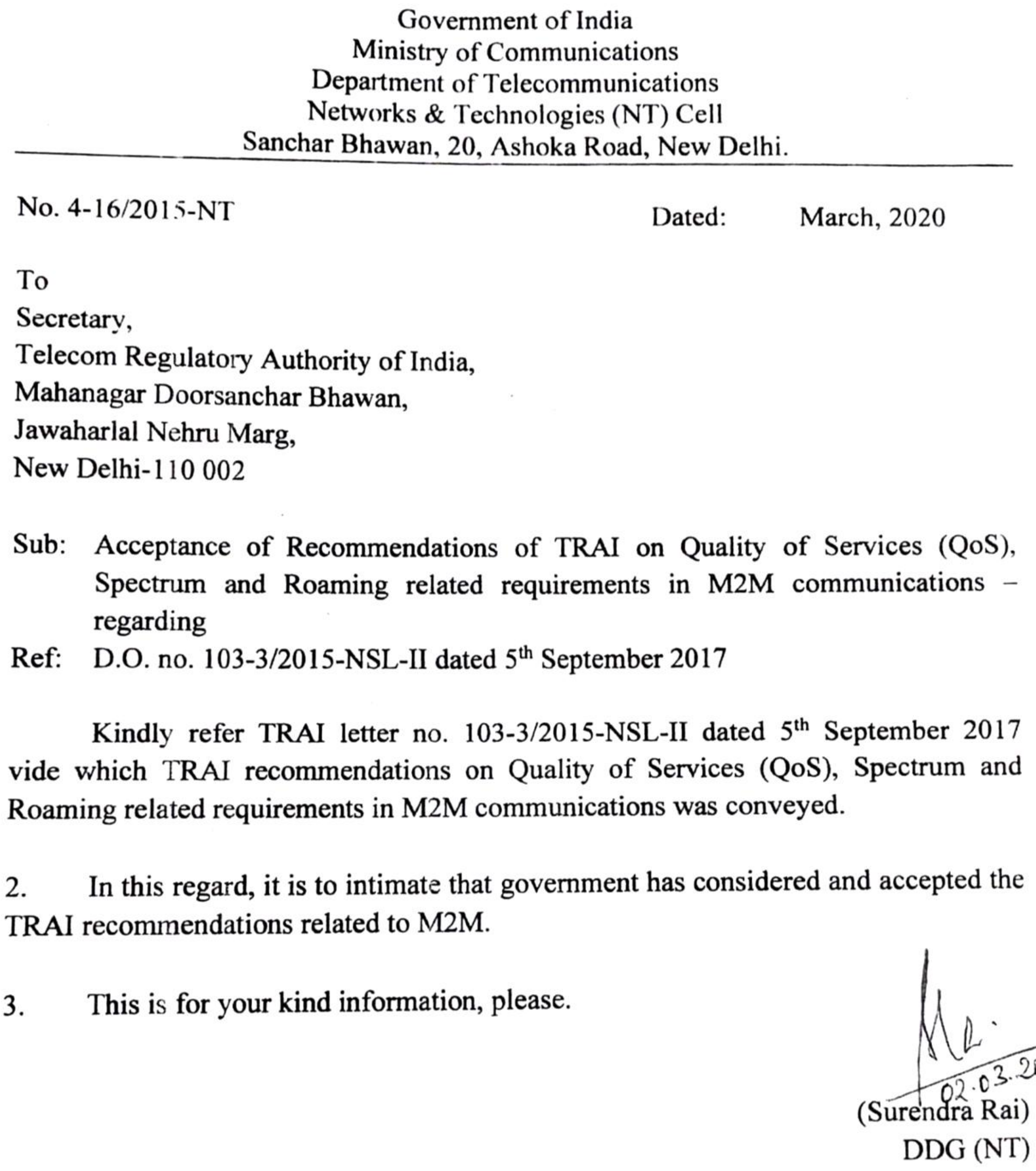
i. Identification of Critical Services in the M2M Sector

ii. Transfer of Ownership of M2M SIMs

Enclosure: As above

(Dindayal Tosniwal)
DDG-NT, DoT HQ
011-23232348

To
The Secretary,
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawaharlal Nehru Marg,
New Delhi-110 002



Government of India
Ministry of Communications
Department of Telecommunications
Networks & Technologies (NT) Cell
Sanchar Bhawan, 20, Ashoka Road, New Delhi.

No. 4-16/2015-NT Dated: March, 2020

To
Secretary,
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawaharlal Nehru Marg,
New Delhi-110 002

Sub: Acceptance of Recommendations of TRAI on Quality of Services (QoS), Spectrum and Roaming related requirements in M2M communications – regarding

Ref: D.O. no. 103-3/2015-NSL-II dated 5th September 2017

Kindly refer TRAI letter no. 103-3/2015-NSL-II dated 5th September 2017 vide which TRAI recommendations on Quality of Services (QoS), Spectrum and Roaming related requirements in M2M communications was conveyed.

2. In this regard, it is to intimate that government has considered and accepted the TRAI recommendations related to M2M.

3. This is for your kind information, please.

02.03.2020
(Surendra Rai)
DDG (NT)

Extracts of the report of the Inter-Ministerial Working Group constituted to identify Critical Services in M2M sector

In order to have wider understanding of the sectorial requirements of critical M2M applications, an Inter-Ministerial Working Group was constituted.

Observations of the Inter-Ministerial Working Group are as below:

a) Critical Internet of Things (IoT) is an emerging concept in IoT development that enables more efficient and innovative services across a wide range of industries by reliably meeting time-critical communication needs.

b) Critical IoT addresses the time-critical communication needs of individuals, enterprises and public institutions. It is intended for time-critical applications that demand data delivery within a specified time duration with required guarantee (reliability) levels.

c) *Failure in a critical IoT system, unlike with massive IoT, could lead to widespread systematic issues within a smart city, business, or infrastructure setting. Critical services thus require high QoS, ultra-reliability, very low latency, very high availability along with accountability with requisite security.*

Recommendations of the Inter-Ministerial Working Group:

The Inter-Ministerial Working Group recommends following services to be classified as Critical M2M/ IoT Services:

i. Connected and Autonomous Cars/ three wheelers and two wheelers

ii. Remote Surgery - 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 and Gas

viii. Safety & Surveillance; State, Commercial and home security monitoring, Surveillance applications, Fire alarm, Police

ix. Defense 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. Distribution Network of inflammable/ explosive articles

xv. Chemical and Nuclear Industry

xvi. Food Industry including Smart Cultivation, Storage and Public Distribution Systems

xvii. Aviation - Remote radar systems

xviii. Drone Communications including UAV-UAV, UAV-GCS and UAV-Network.

xix. Space and Research

xx. Control network of Smart Cities

The regulatory requirements for above identified critical services covers broad range and is to be defined by respective ministries as being done by ARAI and BIS. However broad recommendations of the working group are:

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. Detailed regulatory requirements for these critical services shall be issued by respective ministries/ regulatory bodies.

Annexure-III

The list of stakeholders who have provided comments on the IMWG Report and SLA required for Critical Services is as under-

1. DSP Works (M2M SP)
2. Intellismart (M2M Stakeholder)
3. Itron (M2M Stakeholder)
4. Susan Future Technologies Private limited (M2MSP)
5. Ubiik (M2M Stakeholder)
6. Trilliant (M2M Stakeholder)
7. Boltron (M2M Stakeholder)
8. CESC Limited (DISCOM/M2MSP)
9. Enthutech (M2M Stakeholder)
10. Department of Science and Technology (Govt.)
11. CDoT (Autonomous Body)
12. SIAM (Society of Indian Automobile Manufacturers)
13. Ministry of Commerce (Govt.)
14. TATA Communications (M2MSP)
15. Ministry of Power (Govt.)
16. COAI (Association)
17. Wirepas (Technology Provider)
18. VOICE (Association)
19. Cientra (M2M Stakeholder)
20. LORA alliance -Senra (M2MSP)
21. Sensorise (M2MSP)
22. HAL (PSU)
23. Ministry of Defence (Govt.)

ANNEXURE II

Wireless M2M Technologies

1. Fixed & Short-Range Technologies

(a) **RFID (Radio-Frequency Identification):** RFID networks use radio frequency identification to provide wireless connectivity to M2M devices over short distances. RFID networks can offer low power consumption, cost, and complexity. RFID networks also support passive tags, which do not require batteries or power sources. However, RFID networks have limited bandwidth, range, and security. The use cases and advantages are as given below:

(i) Use Cases: Inventory management, access control.

(ii) Advantages: Contactless identification, low-cost tags.

(b) **Bluetooth:** Bluetooth networks use unlicensed spectrum to provide wireless connectivity to M2M devices over short distances. Bluetooth networks offers low power consumption, cost, and complexity. However, Bluetooth networks also have limited bandwidth, range, and scalability. The use cases and advantages are as given below:

(i) Use Cases: Wearable devices, proximity sensors, smart locks.

(ii) Advantages: Low power consumption, short-range communication

(c) **Zigbee**: Zigbee networks use unlicensed spectrum to provide wireless connectivity to M2M devices over short distances. Zigbee networks can offer low power consumption, cost, and complexity. Zigbee networks also support mesh networking, which can extend the range and reliability of the network. However, Zigbee networks have limited bandwidth, speed, and interoperability. The use cases and advantages are as given below:

(i) Use Cases: Smart lighting, energy management, industrial automation.

(ii) Advantages: Low power consumption, mesh networking, interoperability.

(d) **Wi-Fi**: Wi-Fi networks use unlicensed spectrum to provide wireless connectivity to M2M devices over short distances. Wi-Fi networks can offer high bandwidth, speed, and flexibility. Wi-Fi networks also have limited range, interference, and security issues. The use cases and advantages are as given below:

(i) Use Cases: Home automation, industrial automation, smart buildings.

(ii) Advantages: High data rates, low latency, cost-effectiveness for local deployments.

2. Long Range Technologies (Non-3GPP Standards)

(a) **LoRaWAN (Long Range Wide Area Network):** LoRa is a wireless communication technology developed for Low-Power Wide-Area Networks (LPWANs). It enables long-range communication between remote devices with low power consumption. LoRa operates in unlicensed frequency bands. LoRa is based on CHIRP (Compressed High Intensity Radar Pulse) spread spectrum modulation, which maintains the low power characteristics but significantly increases the communication range enabling a low-cost commercial deployment. The use cases of this technology are:

(i) Use Cases: Smart agriculture, asset tracking, smart cities.

(ii) Advantages: Long-range communication, low power consumption, low-cost infrastructure deployment.

(b) **Sigfox:** In the Sigfox system, low transmissions combined with advanced signal processing techniques provide a high link budget and highly effective protection against interference. Sigfox is based on Ultra Narrow band modulation. Sigfox devices send only a few bytes per day, week, or month in an asynchronous manner and without the need for central coordination, resulting in a single battery life of 10-15 years. The use cases and advantages are as given below:

(i) Use Cases: Smart meters, asset tracking, environmental monitoring.

(ii) Advantages: Ultra-narrowband technology, long-range coverage, low power consumption, low device cost.

3. **Long Range Technologies (3GPP Standards)**: Cellular Networks (3G/4G/ 5G) use licensed spectrum to provide wireless connectivity to M2M devices over long distances. Cellular networks can offer high bandwidth, reliability, security, and global coverage. However, cellular networks also have high power consumption, cost, and complexity. Cellular technologies include 2G, 3G, 4G, and 5G standards, as well as low-power wide-area network (LPWAN) technologies such as NB-IoT and LTE-M1. The use cases and advantages are as given below:

(a) Use Cases: Fleet tracking, remote monitoring, telematics, smart meters.

(b) Advantages: Wide coverage, high data rates, scalability, mobility support.

LIST OF ACRONYMS

Acronyms	Description
AMC	Annual Maintenance Contract
CAF	Customer Agreement Form
CDMA	Code Division Multiple Access
CNPN	Captive Non-Public Network
3GPP	3rd Generation Partnership Project
5G	Fifth generation
DoT	Department of Telecommunications
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
eSIM	Electronic Subscriber Identity Module
ER	Essential Requirements
ESN	Electronic Serial Number
FTTH	Fiber to the Home
GSMA	Groupe Speciale Mobile Association
GSM	Global System for Mobile Communication
ICT	Information and Communications Technology
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IMT-2020	International Mobile Telecommunications-2020
IMWG	Inter-Ministerial Working Group
IoT	Internet of Things
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union’s Telecommunication Standardization Sector

KYC	Know Your Customer
LEA	Law Enforcement Agency
LPWAN	Low Power Wide Area Network
LoRa WAN	Long Range Wide Area Network
LTE	Long Term Evolution
LTE-M	Long Term Evolution for Machines
M2M	Machine To Machine
M2MSP	M2M Service Provider
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
PAN	Personal Area Network
MTCTE	Mandatory Testing and Certification of Telecom Equipment
NCCS	National Centre for Communication Security
NCIIPC	National Critical Information Infrastructure Protection Centre
NOC	No Objection Certificate
NSA	National Security Agency
NSDTS	National Security Directive on Telecom Sector
NTC	National Trust Centre
OEM	Original Equipment Manufacturer
OHD	Open House Discussion
P2P	Person-to-Person
PLC	Power-Line Communications
POS	Point of Sale
QoS	Quality of Service
R&D	Research & Development

RFID	Radio Frequency Identification
RTT	Round Trip Time
SIM	Subscriber Identity Module
SLA	Service Level Agreement
STQC	Standardisation Testing and Quality Certification Directorate
TEC	Telecommunication Engineering Center
TRAI	Telecom Regulatory Authority of India
TSOC	Telecom Security Operation Centre
TSP	Telecom Service Provider
UL	Unified License
UL-M2M	Unified License – Machine to Machine
UL-VNO	Unified License – Virtual Network Operator
V2V	Vehicle-to-vehicle
V2I	Vehicle-to-Infrastructure
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
Wi-Fi	Wireless Fidelity
WLAN	Wireless-Local Area Network
WPAN	Wireless Personal Area Network