

**Government of India
Ministry of Communications
Department of Telecommunications
Networks and Technologies Division
2nd Floor, Door Sanchar Bhawan, JLN Marg, New Delhi -110002**

OFFICE MEMORANDUM

No. 4-31/M2M Critical Services/2019-NT

Dated: 29.07.2025

Subject: Framework and Guidelines for Classification of Critical Services in the M2M/IoT Sector

Kind reference is invited towards the TRAI (Telecom Regulatory Authority of India) recommendations dated 22.04.2025 on "Issues Related to Critical Services in the M2M Sector and the Transfer of ownership of M2M SIMs," which has been by and large accepted by the Government.

2. Brief on Critical Services in the M2M/IoT Sector:

The Machine-to-Machine (M2M) and Internet of Things (IoT) ecosystem encompasses a vast and growing array of applications transforming various sectors. While many of these applications serve to enhance routine functionality and operational efficiency, certain M2M/IoT services are vital as they support critical operations across sectors. These 'critical services' are characterized by their need for uninterrupted, highly secure, and dependable connectivity, often requiring ultra-low latency and exceptionally high availability.

Any failure or disruption in the connectivity supporting these critical M2M/IoT services can lead to significant adverse impact on national security, economy, public health, and public safety.

3. Need for Identification of Critical M2M/IoT Service:

As critical M2M/IoT communications (i.e. ultra-reliable low-latency M2M/IoT connectivity with very high availability) will be used for delivering services of critical importance, the identification of services as critical M2M/IoT service requires to be done well in advance. The identification of a service as critical M2M/IoT service will enable user agencies to enter into suitable service level agreements (SLAs) with the relevant Service Providers. Through the SLAs, the Service Providers may be held accountable for ensuring that the M2M/IoT connectivity provided by them meets the requisite telecommunication service performance parameters (such as latency, reliability and availability) which are essential for the successful operation of concerned critical M2M/IoT service. Therefore, it is imperative to establish a robust framework for identifying and regulating these critical services.

4. This Office Memorandum conveys the framework and provides broad guidelines for the classification of such critical M2M/IoT services to be adhered by all concerned Ministries/Regulatory Bodies, as applicable.

5. Framework for Classification of Critical M2M/IoT Services:

(a) A service (application) shall be classified as 'critical M2M/IoT service' if it satisfies the following twin criteria:

- i. The service (application) demands ultra-reliable, low-latency M2M/IoT connectivity with very high availability.
- ii. Any disruption of the M2M/IoT 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 M2M/IoT sector, specific M2M/IoT services (applications) within the domain/ sector shall be classified as critical M2M/IoT services.

(c) Any M2M/IoT service shall be considered as a non-critical unless identified and notified as critical M2M/IoT service.

(d) The classification of critical M2M/IoT services of a particular domain/ sector shall be done by the ministry/ regulatory body concerned in consultation with DoT. Telecommunication Engineering Centre (TEC), the technical wing of DoT shall be the nodal unit in this regard.

(e) The institutional mechanism for classification of critical M2M/IoT Services is specified in Para 6 of this OM.

(f) Technology Agnostic Approach:

Any wireless M2M/IoT communication technology (utilizing unlicensed spectrum, or licensed spectrum) or wired M2M/IoT communication technology should be permitted to be used for the provision of critical M2M/IoT services, if it meets the prescribed service performance benchmarks (such as latency, reliability, availability etc.).

6. Institutional Mechanism for Classification of Critical M2M/IoT Services:

To facilitate the classification process, an institutional mechanism involving the constitution of a Standing Committee is envisaged:

(a) Constitution: Each concerned Ministry/Regulatory Body is advised to constitute a Standing Committee comprising officers with relevant domain knowledge of the sector

and the M2M/IoT applications related to it. Telecommunication Engineering Centre (TEC), on behalf of DoT, will also nominate one or more officers as members of the Standing Committee and shall assist the concerned Ministries/Regulatory bodies.

(b) Functions: The Standing Committee will be responsible for:

- i. Identifying and recommending specific M2M/IoT services (applications) within their domain/sector that meet the criteria of 'critical M2M/IoT service'.
- ii. Recommending appropriate and measurable service performance benchmarks for each identified critical service. These benchmarks should include parameters such as latency, reliability, availability, and other relevant metrics specific to the service and sector.

7. Notification and Online Repository:

After consideration of the Standing Committee recommendations, the concerned Ministry/Regulatory Body shall notify the regulatory requirements, including the telecommunication service performance benchmarks (such as latency, reliability, availability etc.), for each critical M2M/IoT service separately. The online repository of sector-wise critical M2M/IoT services and their corresponding regulatory requirements, including the notified service performance benchmarks by concerned ministries/regulatory bodies, shall be established and maintained by the Telecommunication Engineering Centre (TEC), DoT.

8. DoT has also notified the Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules, 2025, to establish a regulatory framework ensuring that telecom equipment used in India meet safety, security, and performance standards. As per MTCTE (Mandatory Testing and Certification of Telecom Equipment) framework under these rules, every telecom equipment must undergo mandatory testing & certification prior to sale, import or use in India. In respect of M2M/IoT devices, it has been decided that -

- a. Only the communication modules* of those devices used in critical M2M/IoT services, may be brought under the framework of MTCTE in a phased manner.
- b. Similarly, the communication modules* of those devices used in non-critical M2M/IoT services which may pose threat due to their sheer volume (to be determined by the Standing Committee of the concerned Ministry/Dept.) may also be brought under the framework of MTCTE in a phased manner.

*Communication modules are device agnostic and connect the devices to the telecommunication networks.

9. Ministries/Regulatory bodies are advised to constitute the Standing Committee at the earliest to initiate the process of identifying and recommending critical M2M/IoT services within their respective domains. Ministries/Regulatory Bodies may communicate with Sr. DDG, TEC at srddg.tec@gov.in, 011 - 23320252, 23329088 for further action, including nomination of TEC representative(s) to the Standing Committee.

10. The Department of Telecommunications (DoT), through its technical arm, TEC, is committed to providing all necessary support and technical assistance for the smooth and effective implementation of this framework.



Dindayal Tosniwal

DDG (Networks and Technologies)

Department of Telecommunications

Government of India

E-mail: ddgnt-dot@gov.in

Contact No.: 011-23232348

To:

1. Secretaries of Departments of GoI and Heads of Regulatory Bodies (As per standard list)

Copy To:

1. Sr. DDG, TEC, DoT