VIL Comments to the TRAI Consultation Paper on the "Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs" issued on 24.06.2024

At the outset, we are thankful to the Authority for giving us this opportunity to provide our comments to the TRAI Consultation Paper on "Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs" issued on June 24, 2024.

In this regard, we would like to submit our question-wise comments as follows, for Authority's kind consideration:

Question-wise Comments

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.

VIL Comments to Q1.

1. **TRAI recommendations and Report of *the Inter-ministerial Working Group:***

   a. Basis a detailed consultation, TRAI had recommended in 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."*

   b. These recommendations of TRAI were accepted by DoT and accordingly an Inter-ministerial Working Group was set up that identified 20 services as Critical M2M as given below:

i. Connected Vehicles and Autonomous Cards/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 & Gas and critical infrastructure construction projects
viii. Safety & Surveillance; State, Commercial and home security monitoring, Surveillance applications, Fire alarm, Police
ix. Defence Networks
x. Financial Transactions
xi. Remote early warning sensors – for weather alert and disaster management
xii. Energy Smart Grids
xiii. Utilities distribution networks including Power, Water and Cooking Gas
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

c. The deliberations of the IMG are not available to the stakeholders as such, we request TRAI to kindly share the IMG Report as part of the present consultation, in the interest of transparency.

2. Need for Broad-level Guiding framework for Defining a Service as Critical M2M/IoT service

a. Yes, there is a need for a guiding framework which provides for a standardized approach to define a service as critical M2M/IoT service.

b. The M2M ecosystem represents a future where billions to trillions of everyday objects and the surrounding environment are connected and managed through a range of communicable devices, networks, and cloud-based servers. Such ecosystem will comprise of critical technologies for an optimized air interface, device manageability, network architecture, and security in order to enable future mass deployment of embedded devices. There are multiple use-cases of M2M services however, there are some sectors /services which may succumb to failure if specific requirements in terms of security, network or connectivity are not ensured. It is for this reason that TRAI recommended that such services should be mandated to be provided only by connectivity providers using licensed spectrum.

c. For such critical sectors, as the entire infrastructure and end services are interlinked, as such, there is a need to have uniform approach for treating the entire end to end chain as a critical M2M/IoT service. If some segments are treated as non-critical, it would create isolated islands of connectivity and may undermine the overall safety, security, reliability of the identified Critical M2M/IoT service. **Therefore, in our comments hereinafter, to all questions, the reference to Critical M2M/IoT service, should be read as reference to all segments of infrastructure, application and end service, which is used for delivery of Critical M2M/IoT service to consumers.**

d. DoT, in its letter on "Inviting comments on the identification of Critical Services in M2M sector" dated March 22, 2023, stated as below:

> *"M2M services and applications can be differentiated based on their nature as critical and non-critical. A large number of devices and applications in M2M/IoT ecosystem will be non-critical in nature.* ***However, there would be some critical M2M applications that would require robust, resilient, reliable, redundant and secure networks. Critical M2M applications required ultra-reliability, very low latency, very high availability and accountability."***

e. Such robustness, resilience, reliability and security of the networks needs to be clearly demarcated since any deviation in working of these critical M2M services can cause substantial damage to its users, National security, Resilience of National infrastructure and Delivery of Essential services as well as can also cause serious law and order problems.

f. Highest level of robustness, reliability, availability and accountability can only be made if the end-to-end service (i.e. both infrastructure and end service to users) is provided by licensed entity over licensed spectrum.

g. **Considering the high level of impact which can be caused due to failure of Critical M2M ecosystem, there is a need for a broad guiding framework for defining a service as critical M2M/ IoT service.**

3. Guiding Framework

The guiding framework should be principle based and future fit, providing ample clarity, so that it can cater to all future cases of critical M2M/IoT services which cannot be foreseen at present. In our view, the guiding framework should be based on following pillars:

a. **Guiding principles:** These critical services demand differential treatment as there is a need for end to end support to these services with required quality of services and scalability involved across various layers of network. To make the framework future fit and flexible, there should be guiding principles which can help examine and include new use-case of critical M2M services in future, which are not available at present. In our view, following Guiding principles to define a M2M/IoT service as Critical, should be incorporated in the guiding framework:

   i. Services which support business services and infrastructure which is of important national interest.

   ii. Services whose disruption can lead to serious consequences, significant public inconvenience, and economic loss of revenue for states/enterprises.

   iii. Services which can cause health, safety or environment hazards to the citizens.

b. **Licensed Spectrum usage:**

   i. The most important pillar for the seamless working of the Critical M2M/IoT service is that it should be based on the usage of licensed spectrum.

   ii. TRAI had itself recognized in 2017 that:

   > *"operation in licensed spectrum has certain exclusive rights in terms of usage and is also shielded for any interference. Also, the QoS parameters are measurable and enforceable. Moreover, the government has administrative control over the licensed connectivity providers. So, critical services should be identified and mandated to be provided by connectivity provider using licensed spectrum. 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."*

   iii. Therefore, the Guiding framework should mandate usage of licensed spectrum for delivery of any Critical M2M/IoT service.

c. **Standards and inter-operable systems:** Further, for ensuring reliable and redundancy in the Critical M2M/IoT architecture and devices, it is important that it is based on standards and inter-operable systems. All the smart M2M/IoT services in any critical sector should be inter-operable and not based on proprietary standards and hence it would neither be wise nor desirable to offer any subset of services in a critical sector on unlicensed spectrum.

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.

VIL Comments to Q2.

1. **The recommendations 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. Considering the proliferation of M2M/IoT services, increase in dependency for availing public and essential services and grave cyber security threats being witnessed across the globe, it has become a matter of utmost necessity in national interest, that the said recommendations and the recommendations of the Inter-ministerial Working Group are put for immediate implementation instead of reviewing the same.**

2. **Importance of Use of Licensed Spectrum in Critical M2M Ecosystem:**

   a. The devices and applications using unlicensed spectrum are not put through any of rigorous testing, monitoring, and compliance framework by the Government and thus, have limited security built for data and signaling equipment as also the traffic generated by the devices and applications using the unlicensed spectrum. This makes these systems much more prone to vulnerabilities, threats and cyber-intrusions and if allowed to be implemented in a critical sector/service, can even lead to disruption in operations of critical public infrastructure.

   b. Critical services **have stringent requirements on availability, latency, security, inter-operability and reliability**, which can be offered/ensured only on licensed spectrum.

   c. All the smart M2M/IoT services in any critical sector should be inter-operable and not based on propriety standards and hence, it can have huge impact if any subset of services in a critical sector is allowed to operate through unlicensed spectrum.

   d. Provision of any critical M2M services through the medium of unlicensed spectrum should keep in mind that such entities are not subject to any licensing / regulatory framework encompassing a gamut of compliances to licensing provisions and regulations such as QoS parameters, Tariff Regulations, NSDT compliances, KYC, confidentiality of customer information, Regulatory Audits, Consumer Protection Regulations, emergency services, privacy of communication, lawful monitoring and interception, etc. TSPs are thus regulated on multiple counts like, Trusted device certification, Lawful Interception / CDR / IPDR and all other security conditions; whereas there is no such regulation on unlicensed players.

   e. The need for robust, resilient, reliable, redundant and secure networks for Critical M2M services can only be met through licensed entities using licensed spectrum.

   f. Considering the critical nature of such services which should ensure enforcement and accountability, it is important to either define critical services to be given through licensed spectrum OR unlicensed spectrum holders should also be brought under similar licensing and regulatory framework as is applicable to TSPs.

g. We believe that given the critical nature of these services, the ecosystem should ensure resilient and accountable networks, which can be only based on licensed spectrum use.

3. **National M2M Roadmap:** Attention is this regard is drawn to the National M2M Roadmap, appropriate extract of which are given below for consideration.

   a. In the context of M2M Communication Technologies in Power Sector, it mentions:

   "The successful implementation of smart grids requires a holistic and integrated approach so that communication infrastructure could account for different requirements.
   1. *Broad strategy for the communication network may be suggested as under: Selection of Standards needs to be done carefully as options are large and complex. The goal of achieving scalable, interoperable and secure Smart Grid should be consideration. Guidelines should be developed, including mechanisms for interoperability enforcement and, where appropriate, leverage commercial certification activities.*
   2. *Network Security shall be complied carefully. The BIS standard, IS 3292 – Security Standard for Power Control Systems (currently in RFC stage) focusses on IT security and it is recommended to comply with this standard once this is released.*
   3. *Particular care has to be devoted to the energy efficiency of all components ...*
   4. *Smart Grid is one of the major components in making a smart city, along with other sectors like transportation, health care, water, waste management etc. The common thread enabling the transformation of these sectors to become intelligent is communication, computing and electronics. Hence it is prudent, that shared ICT infrastructures are used across the various sectors.*
   5. *Adopting IP Technology: IP has proved itself in regard to scalability, resilience, and as an open standard. Adopting IPv6 will enable to use the benefits of IP in the Smart Grid."*

   b. Similarly, in case of Smart Water, the Roadmap mentions:

   The broad strategy towards Smart Water deployment can be taken as follows:
   1. ***A common GIS platform and cloud platform shall be planned and established, for use across the various smart activities,*** *which can be used for planning, asset mapping and operational use of smart water project. A shared infrastructure can significantly reduce the requirement of CAPEX to enable smart Water.*
   2. *Evaluate the energy footprint and communication infrastructure required for deploying the smart electronic devices.*
   3. *Install common smart meters on shared communication infrastructure for electricity, water and gas to save costs.*
   4. *Each area is unique, and therefore planning has to be done based on assessment of local conditions and usage pattern.*
   5. ***Adopt open, scalable, interoperable and resilient network architecture*** *with use of IP Technology. Adopting IPv6 will enable to use the benefits of IP in the Smart Water.*

   c. Similar emphasis on open interoperable standards, use of common infrastructure to optimize on capex, use of IPV6 is a common theme across various critical M2M sectors.

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

4. **Energy Smart Grid:** Taking the example of Energy Smart Grid, which is one of the services that has been identified as critical by IMG.

   a. Smart grids are expected to integrate a virtually unlimited number of sensors and meters in the distribution segments, sites and homes to support demand/ response, distributed generation and energy-aware applications; this will produce a huge amount of critical information for grid operation to be collected, exchanged and managed in a trustworthy way, requiring bidirectional flows among different layers.

   b. Security & Reliability: Survivability of the communication network to blackouts is essential to enable automatic and prompt recovery from failures of the electrical grid.

   c. Smart grids need fine-grained security policies that account for data confidentiality and integrity, identification and authentication of data, customers and devices, flexible protection level for specific flows and subscriptions, key management, prevention of traffic analysis, intrusion detection systems, protection against data injection attacks and privacy.

   d. Use of licensed spectrum bands in the Energy Smart Grids should be for end-to-end connectivity to make the system as secure as possible. If at the end point, smart meters are deployed using unlicensed bands for the Data Concentrator Unit (DCU), it will result in a scenario where some of the interconnected subsystems will operate on unlicensed bands while others will be on licensed bands.

   e. The devices and applications used in the Smart Grid need to be from trusted sources and have well defined Security compliances and not be based on proprietary protocols and encryptions.

   f. The Smart Grid needs to be standardized, scalable and inter-operable. For Smart metering it is extremely critical that RF Modem/Devices/NIC communication module are standardised, interoperable and follow open standards and don't get Vendor locked as they may need to securely share data with multiple Govt. and Private Agencies and other applications.

   g. **Thus, Advanced Metering Infrastructure/Smart metering being an integral part of smart grid, also needs to be provided over licensed spectrum.**

   h. If smart meters deployment is done on large scale over unlicensed band, it will not only undermine the security of the Smart Grid - which has been identified as a critical service by the IMWG, but would also lead to huge interference and deterioration of QoS and SLA within each other as well as impact licensed band offered to mobility customers

5. **Battery Management Systems** are responsible for communicating with other Electronic Control Units (ECU) in the vehicles to ensure safety and optimized performance. It is essential that such systems run on licensed bands to ensure end-to-end licensed operations.

6. **Public utility infrastructure** like Smart street light, poles and connected solar panels, Industrial machineries in Smart factories /Industry 4.0 and Robotics should be as secure as possible. Hence, these should be operated on licensed bands as well.

7. **End-to-end security for M2M networks** including Smart Grids:

   a. Utilizing licensed spectrum bands in the M2M networks should be for end-to-end (E2E) connectivity. For example, in a smart grid, if at the end point, smart meters are deployed using unlicensed bands for the Data Concentrator Unit (DCU), it will result in some of the interconnected subsystems operating on unlicensed bands while others will be on licensed bands. Hence, for enabling E2E secured infrastructure, all public utility infrastructure should be operated on licensed bands only using standardized equipment.

   b. Further, even if the M2MSPs (a) take telecom resources including backhaul for WPAN/WLAN from authorized TSPs, or (b) use unlicensed spectrum in the network for the last mile connection or for communication between the smart meters in the mesh topology; still the drawbacks of unlicensed spectrum coupled with vulnerable devices will have a widespread cascading impact on the entire network and will severely compromise the security.

8. It is submitted that all the critical prerequisites mentioned by TRAI in terms of reliability, redundancy, resilience, etc. can only be offered by Licensed Operators who are not only required to comply with the National Security Directive on telecom but are also subject to the regulations and guidelines framed by TRAI and DoT, pertaining to security, quality of service, etc. The internet traffic over the licensed spectrum bands is subjected to continuous monitoring for response to resolution and management of any crisis regarding cyber security in telecom sector.

9. **Considering all above, we submit that only TSPs can offer state of the art ubiquitous services on licensed spectrum, and are best placed to ensure secure, interference free, resilient and inter-operable Critical M2M/IoT services.**

10. **Therefore, the TRAI recommendation 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.**

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.

VIL Comments to Q3.

1. In our view, there is a need to bring critical M2M devices under the Trusted Source / Trusted Product framework.

2. While we believe that standardization of devices and application is important for all IoT applications for scalability, it would be extremely important for critical IoT applications in future as they may need to securely share data with multiple Government and private agencies and other applications.

3. We also suggest that for identified critical IoT services, all aspects need to be secured including device, application and connectivity as any unsecured element may open the path for hacker to make backdoor entry and potentially disrupting the critical services.

4. **International precedence:** In recent years there have been various incidents of cyber-attacks on smart grids/power generation systems which have rendered sectoral infrastructure ineffective. The security incidents clearly demonstrate that critical M2M services like Smart Grid and allied public utility infrastructure should be as secure as possible for protecting critical interests of the nation.

5. **Therefore, we strongly urge the Authority to recommend that M2M devices and applications to be used for critical IoT/ M2M services in India, as and when identified by the Government, should follow standardization of protocols, security, data sharing, authentication, and encryption and interoperability with each other. All such devices being used for critical M2M services should also come under Trusted Sources/Trusted Product framework as defined by the Government.**

Q4. Whether there is a need for establishing a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs? If yes,-
(a) What should be the salient features of such a framework?
(b) In which scenarios, the transfer of ownership of M2M SIMs should be permitted?
(c) What measures should be taken to avoid any misuse of this facility?
(d) What flexibility should be given to a new M2MSP for providing connectivity to the existing customers?
Please provide a detailed response with justifications.

VIL Comments to Q4.

1. **<u>Need for establishing a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs:</u>**

   a. DoT's "Instructions for implementing restrictive feature for SIMs issued only for Machine-to-Machine (M2M) communication Service (M2M SIMs) and related Know Your Customer (KYC) instructions for issuing M2M SIM to entity/organization providing M2M Communication Services under bulk category and instructions for Embedded-IMs (e-SIMs)" dated May 16, 2018 state as below:

      The ownership of all such M2M SIMs shall be with entity/organization providing M2M services. 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.

   b. The afore-mentioned instructions also stated that:

      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.*

c. However, when these instructions were implemented on ground, it was realized that these instructions didn't cater to the need of change in ownership of M2M SIMs in various scenarios, viz.:

   i. *involving merger, acquisitions, hive off/split, takeover of companies.*
   ii. *cases wherein companies wish to transfer the ownership from the parent company to its subsidiaries/ other group companies or vice versa/ and between its subsidiaries/ group companies.*
   iii. *cases wherein M2M service provider is ceasing its operations or is filing for bankruptcy, etc. and the M2M SIMs are required to be either transferred to the new M2M service provider or directly to the company where M2M SIMs are used/ deployed.*
   iv. *cases where the M2M service provider is a VNO and its agreement with its NSO ceases or is terminated.*

d. It is important to note that the M2M SIMs are used for mission critical services also and every effort should be made to enable easy process of change in the ownership of these SIMs. The above-mentioned cases lead to the need of change in ownership of M2M SIMs, to be able to follow these instructions in terms of rights of ownership, responsibility of maintaining the database of customers of M2M SIMs, etc.

e. **Hence, there is a need for laying down simple and clear guidelines allowing for the transfer of ownership of M2M SIMs, given that M2M SIMs are used for various critical services, and embedded SIMs are being used extensively in this sector.**

2. **Key points to be covered in the Guidelines on Transfer of Ownership of M2M SIMs:**

a. A simple digitized process to ensure Ease of Doing Business for all the players in the M2M ecosystem.

b. The process 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 cost.

c. All the terms and conditions pertaining to transfer of M2M SIMs should be mutually agreed upon, including the SLAs and obligations, between the two entities which are involved in the transfer process. The mutual agreement between the two entities may be driven by market forces and there should be no regulatory intervention.

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

3. **Scenarios to be Permitted for Transfer of ownership of M2M SIMs:**

a. **Scenarios:** The transfer of ownership of M2M SIMs should be permitted in all the scenarios listed by DoT in its reference dated January 01, 2024. These scenarios including an additional scenario, are given as below:

   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.*

   iv. *For cases where the M2M service provider may be a VNO and its agreement with its NSO ceases or is terminated, such cases should be treated as an exit from operations and the M2M SIMs should revert to the NSO.*

b. **Both 13-digit and 10-digit M2M SIMs to be covered for ownership change:** For all above cases, the transfer of ownership of M2M SIMs needs to be facilitated for both existing 10-digit M2M SIMs as well as 13-digit M2M SIMs. It has been informed earlier that existing 10-digit M2M SIMs are being continued in some cases on account of non-feasibility of SIM change where M2M devices are deployed in diverse/remote locations, non-feasibility of changes in M2MSP's applications, device/machine compatibility issues with 13-digit M2M SIMs etc. **Therefore, it should be clarified that the process for the transfer of ownership, includes both 10-digit as well as 13-digit M2M SIMs.**

c. Also, transfer of ownership of M2M SIMs from VNO to M2MSP needs to be facilitated, subject to mutual agreement with respective NSO.

4. Measure to avoid any misuse of transfer of ownership of M2M SIMs:

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

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

5. Flexibility to be given to new M2MSP for providing connectivity to Existing Customers:

a. M2M service provider should be allowed to handle the transfer in such a way that deactivation/reactivation of M2M SIM, removal of M2M SIM and re-issuance of new M2M SIM, or IoT device reboot or any explicit action from end-users, should not be required, and M2M SIMs can continue *to operate* with earlier configuration parameters. Thus, in such cases, only the date of transfer along with new organization details are to be updated and subscription should not be forced to go through detach and attach activity as it may result in M2M device going offline.

b. Transfer of ownership should be allowed between inter-circle and intra-circle entities.

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

Q5. Whether there are any other relevant issues relating to M2M/ IoT services sector which require to be addressed at this stage? Please provide a detailed response with justifications.

VIL Comments to Q5.

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

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

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

c. However, the unlicensed entities are not subjected to any of the security obligations applicable for licensed TSPs such as MTCTE and NSDTS, which is even applicable for CNPN licensees who are deploying small private networks or licensed TSPs/ISPs deploying Wi-Fi solutions (unlicensed).

d. They work like full-fledged communication service providers but do not have to pay any revenue share in the form of license fees or even spectrum usage charges to the Government unlike other licensees - ISP, TSP and LPWAN providers (who are offering similar services) which results in a huge loss to the national exchequer.

e. RF Mesh providers are following proprietary protocols and standards and their technology is not interoperable among other RF mesh players. Unmonitored implementation of RF Mesh will lead to severe interference within various ISM applications operating in 865-868 MHz and even with licensed band players.

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

xx-- End of Document --xx