Comments on the TRAI IoT Consultation Paper

1. Industry Requirement

- Enable access to mobile networks with a focus on Quality of Service
- Reasonable and frugal prices for national data access
- Simultaneous / fall back access to alternate machine to machine network technologies such as LoRa, SIGFOX, Z-Wave, WiFi
- One window integrated service to eliminate having to go to many access providers
- Embedded SIM cards with Bootstrap Profile and multiple Operational profiles for enabling manufacturing stage fitment of solderable cards, high QoS in the field and a choice of access providers to eliminate a threat of a single MNO lock-in

2. Value addition from an M2M Service Provider

- M2M enablement requires significant value addition that is distinct from the needs of consumer connections
    - Access from diverse mobile networks [GSM, 3G, WiFi, LoRa]
    - Different type of SIM cards [Industrial Grade, Embedded]
    - Different types of connections [Data only, 2G only, 2G+3G]
    - Secure Connection attributes [Private APN]
    - Secure Messaging for SIM and Device Management
- M2M / IoT applications require technical and service oriented value addition often beyond the capabilities of most mobile operators
    - Subscriptions from two or more MNOs, with a single KYC [preferably an eKYC based on Aadhaar or Digital Certificates]
    - Integrated Device and Application Care
    - Connection Diagnostics [On Net, On Net with GPRS, GMLC based location]
    - Device Heart beat [Interfaces to receive alerts and act on them to re-establish the session / connection]
    - Security [SIM lock, IMEI lock]
    - Remote Device Management
    - Compliance to IoT and M2M standards
    - Compliance to mandate for consumer Data to be resident in data centres in India
    - Compliance to periodic reporting of the Data Connections to DoT with eUICC identity, Device identity, Use case description

3. Role of M2M Service Provider

- Role background
    - M2M Service Provider is an operator agnostic role
    - M2M Service Provider is a network technology agnostic intervention

- M2M Service Provider is NOT necessarily a VNO
- M2M Service Provider is NOT covered under the ambit of OSP registration

- Mandatory Responsibilities
  - Registration with the Department of Telecommunications
  - Compliance to DoT, TEC, TSDSI, IoT and M2M standards
  - Source and integrate Telecom resources from authorized TSPs [mobile and other forms of connectivity] as required for the connected machine
    - Fulfil Machine KYC requirements as recommended in the National M2M Roadmap ["In this scenario, M2M service provider shall get the SIMs issued from TSP after fulfilling requisite KYC norms as required in case of corporate connections. Thus ownership of all such SIMs shall be with M2M service provider"]
    - Enable access to mobile networks with a focus on Quality of Service
    - Reasonable and frugal prices for national data access
    - Simultaneous / fall back access to alternate machine to machine network technologies such as LoRa, SIGFOX, Z-Wave, WiFi
    - Single window integrated service to eliminate device OEMs and Industry players having to go to many access providers
    - Maintain an online Portal for OEM and DoT to access Data regarding the M2M Connections ["National M2M roadmap - name and address should be updated on a secured portal, developed by MSP for this purpose or through other suitable on line mechanisms to TSP by M2M service provider "]
  - Offer Device and Application Care
  - Connection Diagnostics [On Net, On Net with GPRS, GMLC based location]
  - Device Management & Heart beat [Interfaces to receive alerts and act on them to re-establish the session / connection]
  - Security [eSIM, SIM lock, IMEI lock]
  - Mandate for consumer Data to be resident in data centres in India
- M2M Service Provider Rights
  - The registration of the M2M Service Provider must procure it the right to Non-discriminatory access to subscriptions and other network resources from the authorized TSPs [all categories of service providers] at reasonable rates

4. eUICC as an enabler

a. Identification and Marking

- IMSI and IccID from contributing MNOs
- Serial No of the eUICC issued by the M2MSP
- Printed identity to be either the bootstrap IccId or the SIM Serial Number from the M2MSP

b. Issuance process

- M2M Process
  - MSP acquires bootstrap, primary and failover IMSI series from licensed TSPs
  - MSP acquires eUICC cards from a GSMA certified SIM Card vendor
  - MSP develops eUICC as per TEC / ETSI guidelines
  - Secure process between SIM vendor and TSP is not altered
  - MSP undertakes KYC of the User on behalf of the multiple TSPs
  - MSP collects Device and User details on its portals
  - MSP activates and manages subscriptions and service levels
- Retail Customer Process
  - MSP acquires bootstrap series from licensed TSPs
  - MSP acquires eUICC cards from a GSMA certified SIM Card vendor
  - MSP develops eUICC as per TEC / ETSI guidelines
  - MSP supplies bootstrapped cards to device OEM for fitment in devices
  - MSP connects to Aadhaar for OTP authentication of Customers
  - MSP ties up with TSPs for Over the air download of subscriptions
  - MSP collects Device and User details on its portals
  - MSP activates and manages subscriptions and service levels

c. M2M SP eUICC Numbering example

Building the Sensorise QoSIM serial number	Example ONLY	
Requirement of ICCID nomenclature		Sensorise Data
Telecom ID	1-2	89
Country code	3-4	91
Network code	5-7	777
YYMM	8-11	1607
Swtich Config	12	1
Six Digits	13-18	100001
Check	19	3

Section	Para	Extract from Consultation Paper	Sensorise Comment
A	1.31	However, it is noted that DoT/TEC is already working on KYC norms, inter-operability and numbering of M2M devices in consultation with the industry. Therefore, the Authority is not raising these issues for consultation.	KYC should be investigated. Currently the cellular connectivity (which is expected to be at maximum 10% of the M2M connections) has a disadvantage compared to other technologies (such as LPWAN, Wifi, Z-wave, etc) that have no KYC requirements.
A	1.32	In case of change of service provider by a subscriber, the SIM/eUICC provisioning techniques like Over The Air (OTA) are being adopted by many operators across the world.	Noted
A	1.32	The Authority feelsthat in view of the facts mentioned above, there is no apparent requirement of number portability in M2M segment as of now	Noted
A	2.5	Thus for areas activated with M2M services, there is a strong case for use of dedicated network infrastructures and services that are reliable and secure. Thus role of the M2M service providers should not be treated in isolation	Noted
A	2.5	Further, it is necessary that such an entity (MSP) could either be a licensed entity with certain obligations cast upon it or be a registered agency with DoT	Registration should be sufficient at this time. Many future MSP will be small companies, as mentioned in section 2.4, and licensing will be a big obstacle to overcome. For critical services (such as can be correlated to infrastructure (power, water, traffic signs, financial transactions)) a License may already be required for a company to operate in this field, an additional License would not make sense, and for such critical services the License should include any M2M specific aspect.

A	2.7	The National Telecom M2M roadmap envisages to have lightweight regulation towards M2M services and addressing concerns like interface issues with Telecom Service Provider, KYC, security and encryption (for the purpose of lawful interception at TSP level), all M2M service providers utilizing telecom facilities from authorized TSPs should have MSP (M2M service Provider) registration as in case of OSP registration.	Noted
A	2.9	Also many M2M services are supposed to be mission critical in nature in city operations. Therefore the issue for consultation is whether MSP could be a licensed entity with moderately light weight licensing/regulatory requirement or it could be a registered agency with DoT.	See 2.5
A	2.11	For TSPs having access service/ISP license and wanting to provide M2M services as separate service, one alternative could be to amend their license to facilitate M2M services or add a chapter of authorisation in the Unified License for the new licensees.	Sensorise has no Objection to existing TSP having their current license amended to facilitate M2M services, but this must not prevent other actors to become MSP's, nor should they be disadvantaged by licenesing timelines compared to TSP's
A	2.12	For provision of M2M services one option could be adding one chapter in VNO license so that MSP can obtain authorization for M2M services using backend infrastructure of the existing TSPs	Sensorise has not objection to a VNO license allowing M2M services, but it should not be mandatory to either be a VNO or TSP in order to become a MSP

A	2.13	**Q1: What should be the framework for introduction of M2M Service providers in the sector? Should it be through amendment in the existing licenses of access service/ISP license and/or Licensing authorization in the existing Unified License and UL (VNO) license or it should be kept under OSP Category registration? Please provide rationale to your response.**	**Sensorise believes there will be many types of MSP's, as also mentioned in section 2.4 of the paper. Keeping this in mind there will be small players who only need a cellular connection to provide a communication channel between a device and the cloud. For these providers a license would be a barrier, preventing proliferations of new services. For this very reason we believe an "OSP-like" registration would be most beneficial for the ecosystem. For critical services there should be other licenses to operate such services already in place, and is not depending on the type technology chosen for communicaiton (unless where the license specifies otherwise)**
A	2.13	**Q2: In case a licensing framework for MSP is proposed, what should be the Entry Fee, Performance Bank Guarantee (if any) or Financial Bank Guarantee etc? Please provide detailed justification.**	**To assist the M2M/IoT revolution and proliferation, the proposed framework must consider that new services will be created, most often created by new companies. Many of these will have limited means, and large entry fees, bank guarantees may make it impossible to introduce the service in India, and they would have to go outside India to offer new services. This would hamper the creativity and entrepreneurship in this area. A reasonable BG (~ few Lacs) should be sufficient to deter trivial players, whilst ensuring that serious players have a chance to innovate whilst complying to DoT requirements**

A	**2.13**	**Q3: Do you propose any other regulatory framework for M2M other than the options mentioned above? If yes, provide detailed input on your proposal.**	**Sensorise is of the view that India has Licenses in place to protect sensitive areas (such as telecommunication, financial transactions, power grids, healthcare, food handling, etc.), and a separate license for MSP makes little sense, as depending on the service provided an MSP may have to get multiple licenses already. Sensorise would propose an OSP like registration in order to have traceability.**
B	2.25	Delicensed Bands for indoor use: 865-867 MHz	**With Europé being the front runner for device deployments, the prices are getting lowered thanks to the volume. With India on different band local companies can not tap into those volumes as the devices have to be changed. It is desirable if India would consider hamonizing the delicensed bands as to enable the same devices to be used in Europe and India.** **Z-wave: Consider adding European Frequencies** **Europe: EN 300 220 868.40 MHz, 869.85 MHz** **India: CSR 564 (E) 865.20 MHz** **Lora: Consider extending the delizensed band to include 868 MHz** **Europe: 865,20 MHz to 868 MHz** **India: 865 to 867 MHz**

B	2.30	864-869 MHz May be considered for PMRTS and CMRTS.	If Frequency band 864-869 could be delicensed for use in M2M communication with limited power of the transceivers it would greatly help the ecosystem as the same ban would be used in Europe and India, which means devices does not have to be refitted/changed in order to be legal in India. It would extend the current free band one MHz both up and down, most important would be to reach up to 869.85 MHz
B	**2.31**	**Q4: In your opinion what should be the quantum of spectrum required to meet the M2M communications requirement, keeping a horizon of 10 - 15 years? Please justify your answer.**	**Most M2M Subscriptions can do with 2G bandwidths. The numbering and bandwidth requirements should be able to cater to 1 Bn M2M Data Connections**
B	**2.31**	**Q5: Which spectrum bands are more suitable for M2M communication in India including those from the table 2.3 above? Which of these bands can be made delicensed?**	**The 864-869 MHz should be delicensed, already 865-867 is delicnesed for low power devices, and extending it upwards will allow harmonization with European bands for both LAN and WAN use (Z-wave, LoRa and Others)**
B	**2.31**	**Q6: Can a portion of 10MHz centre gap between uplink and down link of the 700 MHz band (FDD) be used for M2M communications as delicensed band for short range applications with some defined parameters? If so, what quantum? Justify your answer with technical feasibility, keeping in mind the interference issues.**	**Sensorise does not have the required skill-set to respond to this question in a meaningful manner.**
C	2.32	There should be a policy framework in place to facilitate seamless operation of such machines when imported to Indian ecosystem.	Roaming as a way to ensure global a global service should not be hindered. Current policy however requires data to be kept within India making these solutions void.
C	2.34	This would mean maintaining country specific inventory at each place of manufacture, leading to very high inventory management costs.	Over the Air download of Subscriptions will allow Indian IMSIs to be downloaded to the connected machines, saving unnecessary inventory

C	2.38	Mobile network codes (MNC) directly available with such service providers can be helpful for their branding and will also help to facilitate their roaming requirements efficiently.	MSP should have the ability to get a MNC, with the embedded UICC the need for a bootstrap subscription in the MSP name is crucial, and should have a Mobile Network Code for this as to be able to identify the UICC even before an Operational (commercial) subscription has been activated by the end-user.
C	2.39	As it would no longer be dependent on the specific package that a mobile operator is prepared to offer, but could change SIM and other settings independently, competition in the marketplace for M2M would be enhanced. Furthermore, switching to a new TSP at any stage would be much simpler and less costly for an MSP because the SIM cards that are installed in the M2M devices would not need physical replacement	For the embedded UICC this is not only desirable, but a necessity. With an embedded UICC a device can be made hermetically sealed, as there is no need to insert or take out the SIM
C	**2.41**	**Q7: In your opinion should national roaming for M2M/IoT devices be free?**	**Roaming tariffs has been a hassle for business people traveling, and also for private people on vacations, there are a multitude of examples where people have been charged thousands of dollars/euro/INR for data services while abroad. Within EU this is now treated as unfeir, and an infringement of free movement within EU and will be removed within EU. For M2M services this should also be free within India as no single MNO has a good enough coverage to manage all of India. Looking at critical services (e-Health, Womens safety, etc) this is vital for ensuring the services can be made available at reasonable prices.**

C	2.41	Q8: In case of M2M devices, should; a) roaming on permanent basis be allowed for foreign SIM/eUICC; or b) Only domestic manufactured SIM/eUICC be allowed? and/or c) there be a timeline/lifecycle of foreign SIMs to be converted into Indian SIMs/eUICC? d) any other option is available? Please explain implications and issues involved in all the above scenarios.	a) Foreign IMSIs will inhibit national control, it is not recommended b) IMSIs issued by an Indian Company should be allowed, the manufacturing of the SIM can be anywhere in the world. eUICC carrying multiple IMSIs - home IMSI and foreign IMSIs - should be allowed. Home IMSIs should be allowed to be used at home country, foreign IMSIs should be alowed in the corresponding foreign land c) the foreign IMSI should be allowed for 30 days, within which time a home IMSI should be activated or downloaded d) As above
C	2.41	Q9: In case permanent roaming of M2M devices having inbuilt foreign SIM is allowed, should the international roaming charges be defined by the Regulator or it should be left to the mutual agreement between the roaming partners?	We do not recommend permanent roaming
C	2.41	Q10: What should be the International roaming policy for machines which can communicate in the M2M ecosystem? Provide detailed answer giving justifications.	Sensorise does not see that a specific policy needs to be set especially for M2M devices and services. It should however be clarified how the Privacy and Security Policy for managing data within India should be enforced for devices that roam out of India
C	2.41	Q11: In order to provide operational and roaming flexibility to MSPs, would it be feasible to allocate separate MNCs to MSPs? What could be the pros and cons of such arrangement?	The M2MSPs will need to take subscriptions from several TSPs and other wireless network providers. The MSP must get a separate series. In the example of the embedded UICC the Operational subscription will not be allocated till the card is sold after manufacturing, so the ICCID on the card for identification should belong to the M2MSP.

D	2.44.III	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 it is learnt that oneM2M 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	existing regulations are sufficient.
D	2.45	For instance, one of the key issues to be noted for hosting of application on cloud is the fact that as per the existing telecom licensing guidelines, subscriber data cannot be taken outside India. However, in cloud computing many of the M2M applications will be hosted on servers located outside India. This poses both a regulatory compliance challenge and data security issue.	Agreed
D	**2.52**	**Q12: Will the existing measures taken for security of networks and data be adequate for security in M2M context too? Please suggest additional measures, if any, for security of networks and data for M2M communication.**	**Existing measures, coupled with the increased reporting and traceability requirements from the M2MSP should be sufficient (Up-dated and online information regarding (i) details of M2M end device i.e. IMEI, ESN etc. (ii) Make, Model, Registration no etc. of the machines (i.e. Cars, Utility Meters, PoS etc.) and (iii) corresponding physical custodian's name and address**

D	2.61	**Q13:** **a) How should the M2M Service providers ensure protection of consumer interest and data privacy of the consumer? Can the issue be dealt in the framework of existing laws?** **b) If not,what changes are proposed in Information Technology Act. 2000 and relevant license conditions to protect the security and privacy of an individual?** **Please comment with justification.**	**India is a security threatened country and it is wise for the policy makers to consider policies that enable security agencies to have access to communication networks and the data exchanged between M2M servers and the M2M devices they are managing.**
E	2.73	**Q14:Is there a need to define different types of SLAs at point of interconnects at various layers of Heterogeneous Networks (HetNets)? What parameters must be considered for defining such SLAs? Please give your comments with justifications.**	**In terms of networks, the M2M SLA for mission critical use cases must mandate access to more than one mobile network. The eUICC can enable this requirement.** **Apart from emergency services and Military services, which both uses dedicated networks, all attempts to defines QoS and reserve bandwidth have failed. The two dominant protocols on Internet is TCP and UDP, both of which where drafted in the late 70's, neither of these have QoS. QoS is handled by each ISP as per their agreements with interconnecting networks. M2M services should not require anything in addition.**
E	2.73	**Q15: What should be the distributed optimal duty cycle to optimise the energy efficiency, end-to-end delay and transmission reliabilityin a M2M network?**	**M2M Networks should be encouraged to package data in 140 byte packets so that the SMS fallback from GSM Data and LWPAN networks can co-exist**
E	2.74	**Q16: Please give your comments on any related matter not covered in this consultation paper.**	**The operational process for eUICC issuance are described as a reference**

III	**3.1.vi**	Remote re-programming of SIM over the air (i.e. OTA provisioning) in order to switch connectivity service provider remotely is likely the key to mitigate the lock-in issue	This is very important for M2M where the lifespan of a device may be up to 15 years (vehicles, energy meters, etc), and the lock-in factor is very important. With embedded cards it becomes even more important as the SIM can not simply be replaced.