DEVELOPING A REGULATORY MECHANISM/LEGISLATIVE DOCUMENT IN RELATION TO STANDARZATION OF M2M & IoT

1.LICENSING AND SPECTRUM MANAGEMANT

Licensing and spectrum management is an important issue for ensuring availability and capacity for IoT communications. IoT devices communicate using a range of different protocols, based on their connectivity requirements and resource constraints. These includeshort-range radio protocols such as ZigBee, Bluetooth and Wi-Fi; mobile phone datanetworks; and in more specialised applications such as traffic infrastructure, longer-rangeradio protocols such as Ultra-Narrow Band (UNB).

To communicate to remote networks, IoT devices may send data via a gateway with a wired(PSTN, Ethernet, power line or DSL) or wireless (2G, 3G, 4G/LTE or UNB) connection to the global Internet or telephony network – or directly over one of these mediums. For consumers, the gateway will often be a smartphone or home wireless router. Businesses will frequently make use of their existing corporate data networks.

In the case of the use of radio technologies, M2M is based on the use of both the licensed and the unlicensed spectrum.The licensed spectrum is linked to mobile connectivity.The unlicensed spectrum is important since M2M economics often impose shared connectivity through concentrators which interface with the public network, grouping transmissions from several M2M devices.At the same time, the use ofthe unlicensed spectrum has significant importance for limiting connectivity costs as in most cases the new technologies will make use of unlicensed spectrum, for instance at 433MHz, 868MHz, or 2.4GHz. They do so along side more traditional technologies such as Bluetooth, WiFi or Zigbee. However, just because spectrum is unlicensed, does not mean that access is unrestricted, except in the most under-regulated markets. In most countries, use of the unlicensed bands has strict rules. There are limitations on factors such as power output, channel spacing and duty cycle (the proportion of the time that a device is sending or receiving). The aim of these restrictions is to ensure that devices do not interfere with each other; devices that are constantly blasting out a high power signal 100% of the time would use up all of the available bandwidth.

Devices communicating over kilometres need access to the 300 MHz to 3GHz spectrum area,while centimetre or millimetre contactless transactions may use near field communications at 13 MHz or EHF bands. It is an undeveloped band of spectrum that can be used in a broad range of products and services on mobile and wireless networks, as it allows for higher data rates up to 10 Gbps, like high speed, point-to-point wireless local area networks (WLANs) and broadband access

Millimeter waves have short range of about a kilometer, millimeter wave travels by line of sight, so its high-frequency wavelengths can be blocked by physical objects like buildings and trees. On the other hand and due to its short wavelengths - ranges from

10 millimeters to 1 millimeter- ; they have high atmospheric attenuation and are absorbed by gases in the atmosphere, which reduces the range and strength of the waves. Rain and humidity can impact performance and reduce signal strength.

High-bandwidth point-to-point communication links are used on millimeter wave ranging from 71 GHz to 76 GHz, 81 GHz to 86 GHz and 92 GHz to 95 GHz, and require a license from many international regulatory authorities. On the other hand some regulators allocate some portions of the mmWave on secondary (unlicensed) bases as short-range data links on 60 GHz millimeter wave. One of the design elements under consideration to enable IMT-2020 to meet high demand is to use millimeter-wave frequencies (between 30 and 300 GHz) to deliver faster, higher- quality services. Since at these frequencies, allocations to the mobile service have a larger bandwidth and the transmission range of millimeter waves is relatively shorter than in lower frequency bands – in the hundreds rather than thousands of meters – mobile network operators may find millimeter waves useful to support the use of small cells in their networks.

Some IoT applications may also make use of AM/FM bands in the VHF range. Telecommunications companies are experimenting withwhite space spectrum to make more use of often-unused spectrum bands, while a USpresidential commission has recommended the development of shared-space technologythat enables government, licensed commercial users, and unlicensed users to cooperativelymake use of a large amount of spectrum. The new spectrum organisation schemes, in addition to the classic schemes,could make it necessary to allow for more flexible shared use of the spectrum, also to optimise theuse of this scarce resource.

	Spectrum usage rights		
	Individual licence	*Shared licence*	*Unlicensed*
"General Purpose" networks that can be used for IoT	*Mobile networks (800 – 900 MHz)*	*To be assessed* *The technological innovations regarding "cognitive radio" and "white spaces" allow for maximising the use of the spectrum also in cases in which the band is partially allocated (and cannot be liberated) and therefore individual licences cannot be issued without limitations*	*WLAN - WiFi (2.4 – 5 GHz)*
IoT dedicated infrastructures	*Mobile network evolutions LTE-MTC, 3GPP-IoT (800 -900 MHz, 2.6 GHz)*		*WLAN -WiFi (2.4 – 5 GHz)* *W-MBUS (169 MHz)*

Source: AGCOM

Figure 1.1 Feasible policies for regulating spectrum use

Globally, the trend is to use telecom network of TSP and/ or free wireless bands in non-TSP frequency domains for M2M communications. In India also, de-licensed free bands are available in various frequency ranges, which can be used for M2M communication, as below:

1. Use of low power wireless equipment in the Citizen Band 26.957-27.383MHz with 5 Watt Effective Radiated Power and built-in antenna.
2. Use of low power wireless equipment in the 335MHz band at frequencies 335.7125, 335.7375, 335.7625, 335.7875, 335.8125, 335.8375 MHz with Inbuilt Antenna and up to1 m W transmit power.
3. Use of low power wireless equipment in the 433-434 MHz with 10 m W of Maximum Effective Radiated Power and 10 kHz channel bandwidth.
4. Networks using low power wireless equipment in the frequency band 865-867MHz for RFID or any other device with maximum 1 Watt transmitter power, 4 Watts Effective Radiated Power and 200 kHz carrier bandwidth.
5. Wi-Fi based network in the frequency band 2.4 GHz to 2.4835GHz for Indoor use as well as to access in short range with 4 W of Maximum Effective Radiated Power and up to 5 meters above the rooftop antenna.
6. M2M network for indoor or campus use in the frequency band 5.150 to 5.350 GHz and 5.725 to 5.875 GHz for built-in or Indoor antenna with Maximum mean Effective Isotropic Radiated Power of 200 mW and a maximum mean Effective Isotropic Radiated Power density of 10 mW/ MHz in any 1 MHz bandwidth.
7. M2M network for outdoor use in the frequency band of 5.825-5.875GHz with 4 W peak ofMaximum Effective Isotropic Radiated Power.

Telecom Regulatory Authority of India (Trai) in its recommendations on "spectrum, roaming and quality of service related requirements in M2M communications" said spectrum allocation should be technology and service neutral and no separate spectrum band should be allocated exclusively for M2M services.However, in order to facilitate the smooth roll-out of M2M services utilising "licence exempt spectrum, 1 MHz of spectrum at 868 MHz (867-868) and a chunk of 6 MHz of spectrum at 915-935 MHz is recommended to be delicensed. Delicensng the V-band (57-64 GHz) as recommended by the authority on various occasions may be done on priority."

Studies for the European Commission have suggested that a licence exempt model is mosteffective for IoT development, since it avoids the need for contractual negotiations beforedevices are manufactured and used, allowing the production of large numbers of cheap devices. Most current systems use unlicensed frequencies in the Industrial, Scientific andMedical (ISM) bands, including sub-kHz for video surveillance and access control, theMedical Implant Communications Service (MICS) in the 400 MHz band, and 900 MHz for theEPC RFID standard. The generic Bluetooth, ZigBee and Wi-Fi standards also work in unlicensed spectrum.One example of a specific long-distance IoT-focused communications system, SIGFOX, usesthe most popular European ISM band (the ETSI and CEPT-defined 868MHz) and the FCC-defined 902MHz band in the

USA. A Korean government review found an increasingdemand for unlicensed, low-power, long distance communications to connect devices in remote areas.

Examples of internationally frequency bands which are under study to be allocated on harmonization basis are the following frequency bands:

Frequencies under study on secondary basis (shared /SRD/ low power/ISM) For technologies such as ZiGBee , Bluetooth, RLAN 811.11n,811.11af	Frequencies under study on primary basis For technologies such as :EC-GSM-IoT ,NB-IoT , LTE-M
164 - 169.8152 MHz	410-430/450-470 MHz
433.05 - 434.79 MHz	703-733/758-788 MHz
862-863 MHz	791-821/832-862 MHz
863-870 MHz	880-925/832-868 MHz
870-876 MHz	1452-1492 MHz
915-921 MHz	1710-1785/1805-1880 MHz
1880-1900 MHz	1920-1980/2110-2170 MHz
1900-1920 MHz	2300-2400 MHz
2400-2485,3 MHz	2500-2570/2620-2690 MHz
5150-5350 MHz	2570-2620 MHz
5470-5725 MHz	3400-3600 MHz
5725-5875 MHz	3600-3800 MHz
61-61.5	
57-66 GHz	
57-64 GHZ	

It understands that in all cases standardization of technologies (and harmonization of frequency bands) is required for interoperability and compatibility reasons. However,

Nepal will consider technology neutrality as no single standard will be able to cover all IoT/M2M cases due to the enormous variety of applications.

It is expected that both wired and wireless solutions will able to meet backhaul demands in the market. Various technical solutions could be considered by the operators to facilitate backhaul roll out and to meet the traffic needs such as optical fiber or wireless links. Alternative technologies such as xDSL cable based backhaul also expected to be viable alternatives.

According to the current networks and IoT technologies wireless backhaul requirements and demands can be fulfilled in the short and mid –term by the current frequency bands applying the currently available spectrum efficient techniques. In the long term, according to the market demand regulatory body will consider if new frequency bands might needed for backhaul applications and channel plans that could support the use of broadband radio systems

Recommendation

It is recommended that Nepal

- Develops its own Spectrum Management Strategy.
- All existing telecom service providers(TSPs) can be allowed to provide Machine-to-Machine (M2M) or IoT solutions within their specified circle of operations, if they wish to provide M2M/IoT VAS services.
- All the license holders can use existing spectrum to provide IoT services
- An M2M/IoT VASservice provider(MSP) can also be a telecom service provider and could also provide services for both enterprises and home users.
- Individual M2M/IoT VAS service providers(MSPs) should register with NTA and declare their TSP partnerships formed for connectivity to their M2M application.
- Exclusive guidelines for MSP Registration should be issued.
- The government, through NTA, should identify critical services and differentiate them from non-critical services. IoT and M2M applications in healthcare, remote surgery, driverless cars etc. require high QoS, ultra reliability, very low latency, very high availability and accountability. Therefore, these critical services should be provided only by “robust wired optical fiber, copper network or LTE capable access networks.
- Industry regulators (apart from NTA) such as Nepal Bureau of Standards and Metrology and the Department of Drug Administration[1] need to constitute their own regulations and policies regarding M2M and IoT solutions.

[1]https://www.export.gov/article?id=Nepal-Trade-Standards

- For Spectrum availability, usage and SIM requirements,
    - Spectrum allocation should be technology and service neutral
    - No separate spectrum band should be allocated exclusively for M2M services, unless it is for a very critical service or sector such as defence.

- Requirement of fresh spectrum:
    - Requirement of additional licensed spectrum for access services to meet the projected influx of connected devices due to M2M communication needs to be studied by NTA once the momentum for adoption picks up in the country.
- Imported SIM cards can be allowed for M2M/IoT
    - It should not be mandatory to use only domestically manufactured SIMs in M2M.
    - Embedded SIMs with standard specifications can be imported and relevant information shall be submitted by importer while import of the devices/SIMs

2. SWITCHING AND ROAMING

Firms operating large networks of M2M devices via mobile telephony networks, with a fixed SIM in each device, may not find it easy to switch network at the end of a contract, or if a device roams into a different network area or for some time period could get better service from a different provider. This roaming capability is important for devices that move between countries, and also for fixed location devices that may be used in an area of short or long periods of service unavailability – often indoors.

Mobile number Portability (MNP) is a service through which customers can switch from one operator to another, keeping their original mobile number. Customers can easily select the network of their choice and don't have to panic for loosing their mobile number.

As the appointment of consultant is in the process, we can assume that the Mobile number portability will be available in Nepal only in 2018.

In the M2M environment where a customer may have thousands or even tens of thousands of widely dispersed devices switching SIM cards in order to changeservice provider is not a viable solution given the cost, effort and time scale involved in visiting each device. A wide range of M2M applications is emerging. These include utility Smart Metering for which there is a single customer (i.e. the utility company) but with potentially millions of end user devices. Under current arrangements, if the utility company wishes to change network operator (e.g. for commercial reasons) it would need to change the SIM cards in millions of devices. That is clearly not a practical solution, as every smart meter would need to be visited to have its SIM swapped out.

The promotion of competition is a regulatory objective to ensure a vibrant market in M2M services and other solutions are needed to avoid “operator tie-in”. These require M2M devices to have IMSI numbers that are independent of the underlying mobile network operators.

Given the nature of M2M applications there may not be the same need to ensure that numbers can be ported when switching service providers.To achieve economies of scale, the manufacturers of M2M devices would undoubtedly prefer to install the M2M identification functionality at the point of manufacture and not have to provision country-specific SIM modules after devices reach their national points of distribution in the market place. A number of different solutions could be considered to meet this need and to facilitate more seamless switching between service providers. One possible solution could be Shared MCC and National Roaming

The ITU designated the MCC 901 as a shared MCC. This allows for the provision of Mobile Network Codes (MNCs) that are not tied to any one national market. Service providers that qualify for an MNC under MCC 901 are able to operate cross-border services using a single SIM with a single price for data connectivity. Some MSPs appear to have found this approach to be beneficial, as it allows SIM functionality to be configured in devices at the point of manufacture. It also allows MSPs to negotiate agreements with several mobile network operators on either a national or an international roaming basis. This approach requires some co-ordination at the international level with the ITU. Efficient management of such a scheme might best be handled by the direct allocation of MNCs and their own blocks of numbers to such very large entities.

MSPs could be at something of a disadvantage by not having MNCs when seeking to negotiate commercial contracts with mobile providers. Acquiring its own MNC (whether a national MNC or a shared international one), could provide more negotiating power to MSPs when agreeing contracts with mobile providers and in relation to roaming agreements. Such agreements could facilitate commercially viable communications coverage within remote regions.

MSPs equipped with their own MNCs could be better placed to completeviable roaming agreements with as many different mobile providers as necessary to achieve full coverage at competitive prices.Opening up access to MNC’s could stimulate competition by enabling balanced negotiations that promote the growth of M2M. A large MSP holding its own MNC could have more leverage when entering negotiations with a potential partner MNO/TSP over its roaming (and other) rates. 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 over the air, competition in the marketplace for M2M would be enhanced. Furthermore, switching to a new MNO at any stage would be much simpler and less costly for an MSP because theSIM cards themselves that are installed in the M2M devices would not need replacing.[2]

[2] An Coimisiún um Rialáil Cumarsáide Commission for Communications Regulation, Consultation Reference: ComReg 13/33 Date: 28 March 2013

3. ADDRESSING AND NUMBERING

A national numbering plan has been in place in Nepal since Subscriber Trunk Dialing (STD) was introduced in the early 1980s for fixed telephone service. The GSM and CDMA mobile numbering plan consisting of 10 national significant digits starting from 96-XXXXXXXX to 98-XXXXXXXX are in implementation.

According to Machina Research, one third of M2M connections are expected to be mobile, with a minority using fixed-line solutions. Given that there is expected to be far more mobile devices. However, it has to be sensitized that the proliferation of M2M services on existing voice numbers could deplete that numbering resource, subsequently resulting in very costly disruption and a difficult and costly task of migrating large numbers of developed M2M services onto a new range.

Also, utilising mobile networks for M2M services will require each communicatingM2M device to have the capability to attach to an available mobile network,there by requiring SIM functionality in all addressable M2M devices. This raises some challenges in the context of number portability and switching between service providers.

In the future IoT, are to be addressed and controlled via the Internet, things should be have just like normal Internet nodes. In other words, they should have an IP address and use the Internet Protocol (IP) for communicating with other smart objects and network nodes. And due to the large number of addresses required, they should use the new IPv6 version with 128 bit addresses. Preferring migration to IPv6 to be widely used for addressing issues especially for critical IoT services instead of its limited size predecessor, IPv4.

IPv6 offers a highly scalable address scheme. It provides 2128 unique addresses, which represents 3.4 × 1038 addresses. It is quite sufficient to address the needs of any present and future communicating device. The total number of possible IPv6 addresses is more than 7.9×1028 times as many as IPv4, which uses 32-bit addresses and provides approximately 4.3 billion addresses.

IPv6 provides many technical benefits in addition to a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables. It provides strong features and solutions to support mobility of end-nodes, as well as mobility of the routing nodes of the network

The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device security and configuration aspects have been considered in the design of the protocol.

Recommendation

It is recommended that for M2M numbering, a national advisory body should be constituted. The Advisory body need to delibrate on issues on M2M numbering challenge, such as,

- **The number of digits** to be used for M2M numbers. The new number range should be as long as is reasonable. This would avoid the need for future expansion of the range to meet a later scarcity of capacity. According to ITU-T recommendation E.164, the maximum permissible number length is 15 digits. EU countries that have already designated number ranges for M2M have generally adopted a 10 or 11 digit format for their M2M subscriber numbers, leading to national capacities of 10 or 100 billion M2M numbers, respectively. In India, the DoT had issued a directive to TSPs mentioning the implementation of 13-digit numbering scheme for M2M communication. Migration of existing l0-digit M2M numbers to 13 digits will start latest by October 1, 2018 and shall be completed by December 31, 2018. All new M2M mobile connections will be allocated l3-digit numbers from July 1, 2018. The DoT has also asked the MSPs to ensure that their network elements including IT and other relevant systems are aligned with 13-digit numbering for M2M SIMs before July 1, 2018.

- **Number Addressing:** The E.164 numbering resources (i.e. numbers in the national numbering plan) are the most viable solution for addressing M2M applications at least in the short and medium run. It is expected that most M2M applications will be based on mobile networks, and therefore within E.164 numbers the present mobile number ranges seem to be most suitable for M2M solutions.As a long term solution IPv6 addresses, or numbers/addresses other than E.164 numbers should preferably be used for device based communication applications. These numbering/addressing schemes or switching from E.164 numbering plan to a new plan should not prohibit market development or competition.

- Whether or not **separate ranges** are required for different types of M2M applications?

  There are possible situations where a new number range should be opened. For example, the number range in question may require different regulatory treatment, such as, relating access to emergency services, or the services to be provided have certain characteristics (e.g. M2M applications in fixed networks) where existing mobile number ranges may not be adequate.

Currently, it is difficult to predict future business models or interconnection regimes, therefore it would be prudent to initially breakdown such a dedicated M2M range into a limited set of sub-ranges for mobile and for fixed applications and also keep open the option for premium M2M. This could provide efficiencies with respect to routing and billing for users.

As some existing regulatory requirements (e.g. access to emergency services) maynot be relevant or useful for M2M applications, exceptions regarding existing regulatory requirements could be applied to new numbering range(s)accommodating these applications.

- **National roaming** for M2M/ IoT shall be under forbearance and the rates can be set under current Telecom Tariff Orders (TTOs) for access service (voice/data) license holders. NTA should review and issue separate Telecom Tariff Orders (TTOs) for M2M and IoT providers at an appropriate time in future, if and when deemed fit.
- **Sharing arrangements**: TSPs (who want to provide IoT/M2M) can separately enter into commercial agreements to meet their roaming requirements for subscribers within Nepal and outside Nepal.

a. COMPETITION

The entry of a new player in telecom market has intensified the competition and forced the incumbent operators to reduce the rates drastically. New bundled plans are being offered with minuscule chargesfor voice calls or completely unlimited voice calls. Also, data roaming in thecountry is not charged by many TSPs for their subscribers. In thecompetitive environment many TSPs has done away with national roaming charges to their subscribers.

As such roaming in M2M will be required mostly by enterprise segment in M2M and possible tariff plans would be of bulk bundled nature rather than usage based as in today's environment. We must be aware of the fact that Average revenue per connection(ARPC) in M2M is comparatively very less as compared to the existing Average revenue per user (ARPU).

As for the licensing regime for M2M, the industry players believe that M2M/IoT services are the application services which will ride on the access services/internet access being provided by the TSPs and ISPs respectively. M2M is inherently a global business which requires regulatory policies to reflect the global essence and recognize as well as facilitate cross borderdata flow amongst many other requirements. There are inherent restrictions in voice related licensing framework, which do not always permit free flow of cross border data. Moreover, Machina Research in 2016has projected that by 2021

there will be merely 8.4% connected devices oncellular connectivity. Since cellular connectivity is projected to be a by smally 8.4%, therefore there is no merit in placing M2M services undera license. Also, M2M services have very low ARPU. License has hugefinancial entry cost, recurring license fee and spectrum charges coupled with bank guarantee cost will make the M2M business financially unviable.

Requiring MSPs to obtain a Unified License or VNO licensewould result in a regulatory imbalance and a disincentive for efficient deployment of M2M services. Licensing will prevent the entry of newservice providers in the M2M space due to inherent advantages ofincumbent providers, thus leading to less competition for existing TSPs& ISPs.

Also, any decision to mandate that all IoT services must use specific, dedicated licensed or unlicensed spectrumwould damage market competition, struggle to meet all IoT use cases, and may lead to services which are not commercially viable.

Recommendation

- Opening up access to Mobile Numbering Codes (MNCs) could stimulate competition by enabling balanced negotiations that promote growth of M2M. Large MSP holding its own MNC could have more leverage when entering into negotiation with potential TSP partner over its roaming and other rates. This would enable the user to be no longer dependent on a specific TSP. This will provide him the freedom/choice to change the SIM and other settings independently, thereby enhancing competition in the market for M2M.
- Applying any fee to obtain Unified License or VNO license for MSPs would act as market entry barrier for new MSP players and would be advantageous to incumbent providers, which may lead to expensive IoT services due to less competition in the market.
- Consumers should have the ability to choose between competing service providers on the basis of being able to compare performance differences in a transparent way. The high degree of competition in the mobile market provides ample incentives to ensure customers enjoy the benefits of an open internet.

- Dedicated licensed or unlicensed spectrum should not be pushed by regulators as different IoT use cases have different spectrum requirements.

b. SECURITY AND PRIVACY

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.

IoT devices are typically wireless and may be located in public places. Wireless communication in today's Internet is typically made more secure through encryption. Encryption is also seen as key for ensuring information security in the IoT. However, many IoT devices are not currently powerful enough to support robust encryption. To enable encryption on the IoT, algorithms need to be made more efficient and less energy consuming, and efficient key distribution schemes are needed.
Managing security and privacy issues has the goal of significantly reduce security problems in IoT systems that let attacker's access private data and cause physical harm in cases such as medical devices and connected vehicles and many other. Such management can be achieved by many practices like: ensuring security and vulnerability patching of devices and of the whole IoT system design process, ensuring individual control of profiles, development of co-regulation to protect security and privacy of personal data with more cooperation between telecom companies, telecom regulators and other related parties.
Some Companies have identified challenges within IoT Systems:
Efficient Encryption algorithms running IoT devices and networks need higher processing power. (Low CPU power vs effective encryption).
Small, inexpensive devices with little to no physical security: Traditional security approaches used in electronic communications may be not sufficient to address low cost devices used by many IoT services.
Crypto algorithms have a limited lifetime before they are broken, which may outlive the original running application. Authenticating to multiple networks securely. Data availability to multiple collectors synchronously and securely.

Manage Privacy concerns between multiple consumers. In which a consumer can utilize multi-vendor service that does not necessarily designed to interact nor comply with each other. The attack surface is dramatically increased; an extensive leverage of open networks will be exposed.

Without adequate security, intruders can break into IoT systems and networks, accessing potentially sensitive personal information about users, and using vulnerable devices to attack local networks and devices, providing a potential route for further attacks among other networks.

Security within IoT Systems includes Software and hardware, software platforms managing devices and running devices firmware, hardware includes IoT devices, network infrastructure, and sensoring equipment.

As the number of “Things” starts to outnumber humans, it will be beyond humans alone to fight security threats, and from a regulator’s point of view, comparing Network-based security solutions with device-based security solutions will be the initial step for securing IoT in general.
Main problem with device-based is that they don’t have the processing power nor the storage capacity to run a comprehensive security protection against threats, thus leading to total network-based security solution, which also may be hard to implement or afford in terms of cost.

Layers of security for Internet of Things, as shown in below table

No.	Security Layer	Security Considerations
1	Physical devices ,endpoint equipment security	• Disabling external device connectivity, and allowing external devices only upon approval, • Review and scanning. • Disabling direct internet access from sensitive devices /endpoints if not required. • Ensuring that unused services are disabled or blocked such as open ports and insecure • Protocols. • Secure firmware booting. • Device secure authentication • Applying regular patches • Device encryption
2	Gateway & Network Security	• Ensuring that IoT/M2M gateway is secure by using appropriate IPS, and filtering • Mechanisms. • Facilities should have adequate physical security such as guards, access cards, visitor • Logs, CCTV CAMs to prevent unauthorized access. • Service providers should obtain and produce assurance certifications such as ISO 27001. • Usage of secure communication channels such as Encrypted VPN for Remote access. • Protecting Web-facing Cloud Services with IPS.

		• Enforcing authentications and encryptions for Wireless communications.

Privacy

As more and more objects become traceable through IoT, threats to personal privacy become more serious. In addition securing data is important to make sure that it doesn't fall into the wrong hands, issues of data ownership need to be addressed in order to ensure that users feel comfortable participating in the IoT.

The ownership of data collected from smart objects must be clearly established. The data owner must be assured that the data will not be used without his/her consent (consumer awareness), particularly when the data will be shared. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal Information, as for regulating Data privacy issue,

Security in this sector is essentially of two types' viz. data security & privacy and device security. While security by design should be embedded in all applications, software and hardware to be used. NTA or an appropriate authority would need to provide appropriate framework for

a) Data Protection, Ownership, Data Security & Privacy
b) Local Manufacturing of Devices including M2M/IoT sensors & local SIMs, etc

Recommendation

- **"Security by design"** principle needs to be implemented and for this, NTA along with the regulatory body for manufacturing sector needs to create fresh guidelines for manufacturing M2M/IoT devices in Nepal Similarly, guidelines for importing M2M/IoT devices in Nepal needs to be created by NTA in consultation with The Nepal Bureau of Standards and Metrology (NBSM).

  MSP shall try to incorporate in overall service design to the extent possible as under:

  i. To the extent possible, only point to point data, SMS and voices services to predefined numbers only shall be enabled on M2M SIM.
  ii. Enable security of Embedded Sensors to protect from computer worms, viruses or other Malware by implementation of security features like e. g. MILS (Multiple Independent Levels of SECURITY AND SAFETY.
  iii. Additional security in sensors may be incorporated by IMEI & SIM PAIR LOCKING so that sensor shall work with the SIM configured by MSP. However the reverse is not encouraged i.e. locking by TSP as it will unnecessarily bind MSP with TSP.

These guidelines should look “the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities.” At the same time, “low-risk” IoT devices (like LED bulbs) need not be burdened with too much regulation, so the government could look at creating a “graded” level of security certification for devices.

Standards for IoT and M2M systems: Since most of the M2M applications “would be operating in (an) unlicensed band, the government should issue specific standards for devices to be used in the M2M ecosystem, in line with international standards organizations.

- To obtain the best-in-class services, it is advised to follow global standards & best practices in this field instead of devising country specific standards/guidelines.

- NTA has to device guidelines for setting up an independent IoT/M2M certification body which certifies both hardware quality and software segments and will be responsible for governance and auditing of all M2M/IoT networks and devices.

- Managing M2M data within TSPs 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 of Nepal.
  - 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 Law Enforcement Agency shall also be applicable in case of M2M service

c. OTHERS

4. Energy Footprint of M2M Networks

There are going to be many devices in terms of sensors, network equipment and data centers to create the communication infrastructures and host servers for M2M services. All these equipment also consume energy. The energy footprint of all these elements could be huge. Hence while designing the M2M networks; it is important to ensure that low power devices are planned so that the Energy footprint is kept to the minimum.

The energy footprint of existing ICT devices is non-negligible, and it is expected to grow over the next years. The additional deployment of sensors, networking equipment and computing devices would just raise future energy requirements. The huge number of such installations boosts very few additional watts in each location but at the scale of a nation, it consumes a huge amount of energy equivalent to the energy produced by several mid-size power plants. Globally several techniques are under study to lower the consumption of ICT devices, based on three main statements:

1. Silicon efficiency grows about half the rate of the capacity of new devices,
2. Power consumption does not linearly follow computational load,
3. Devices are often “on” just to maintain their presence in the network.

Recommendation

It would be wise to put regulations in place on the carbon footprint of M2M devices and standards developed for same so that device OEMS can comply with corresponding regulations.

In addition, the Government of Nepal must work closely with the NTA to ensure that Nepal builds a favorable environment for IoT growth.

5. Key areas of focus for accelerating IoT growth in Nepal

i. **Indigenous products & services** - Indigenous manufacturing of telecom equipment with a preferential treatment to indigenous manufacturers will help Nepal build a strong indigenous industry for IoT. For M2M products, local manufacturing and service is mainly being done by Start ups and SMEs. Basic components like modules, silicon chips and sensors are mostly imported. NTA needs to plan on taking a number of initiatives to promote local manufacturing in M2M domain such as, easy financing, tax benefits, reduced raw material import duties, encourage investment in R&D and IPR etc.

ii. **Creating test bed facilities**–Make provisions and dedicate funds for supporting infrastructure requirements for M2M in terms of test labs, test beds, product certification. Create a test infrastructure for conducting conformance, performance, functional and interoperability tests among public networks and to benchmark devices, applications, networks, services for all real life scenarios. Upgrade the existing facilities for M2M requirements.

iii. **M2M product certifications** - Network device certification is a must-have requirement to bring any new device into existing carrier networks. The EU GCF (Global Certification Forum) was founded in 1999 bringing together leading mobile

network operators, device manufacturers and other stakeholders, to test and certify all new mobile devices with Certification Criteria based on 3GPP and 3GPP2 standards which shall ensure that the mobile device shall work effectively on mobile networks anywhere in the world.

NTA can consider signing cooperation agreement with GCF to take care of Nepal specific requirements in global certification. GCF is also working to engage with industry groups to make GCF certification complement sector specific certification requirements. Other M2M device certification bodies have also been formed like PTCRB in USA, KORE telematics, Telefonica Global M2M module certification program. In India TEC publishes a large number of standards - GR (generic requirements), IR (interface requirements) and SR (service requirements) for communication products and also does product certifications under Interface approval, Type approval and Certificate of Approval for telecom products. For M2M product certifications, existing facilities of NTA may be upgraded and more facilities may be added in CABs (Conformity assessment bodies) and CBs (Certification bodies) as per industry requirements.

iv. **Human resource and Capacity building**–

To train/skill human resource and capacity building for M2M, NTA must invest in building training institutes and incentivise existing technical universities in the country to develop suitable training courses and demonstration centres for M2M. As M2M is across domains, NTA needs to have technical collaboration with Capacity Building centres across industries.

v. **M2M Pilots** - The government had announced its plan to develop Kathmandu Valley, Lumbini Region and Nijgadh as the country's first three smart cities. The government had also allocated NRs 440 million for infrastructure development of 10 modern cities across mid-hill highway. The government has planned to develop and implement a master plan for developing a smart city in the surrounding areas of Marsyangdi with Palungtar of Gorkha at the center of the city. Moreover, the government also has plans to invest in developing necessary infrastructures for converting over a dozen cities – including Walling and Dandeldhura – into smart cities. It is important that pilot projects are carefully thought of and planned well with the role of IoT defined at each stage in the strategy itself.

vi. **Center of Innovation** - Setting up of CoI (Center of Innovation) to develop experimental M2M networks, implement M2M pilot projects, promote R&D for M2M as well as coordination amongst various government bodies, regulators and standards bodies would go a long way in accelerating IoT growth in Nepal.

vii. **Encouraging entrepreneurs and start-ups** - To promote entrepreneurs and start-ups, industry associations would have to take a lead and closely work with government. Relevant Ministries need to work with NTA for taking initiatives to support start-ups by setting up incubation centers to support innovations and R&D.

viii. **To evolve new M2M business models** - From the communication perspective, the following business models can be build by a M2M/IoT VAS service provider (MSP):

a) MSP focuses on its own services, leaves choice of connectivity/network on end customer allowing them to choose TSP of their choice

b) MSP becomes bulk customer of a TSP and provides end to end service along with SIM and connectivity to end customer. He settles bills of TSP as a bulk customer and raises single bill to his customers for overall service including telecom services.

c) A TSP is also a MSP and sells services to customer similar to value added services MSP becomes an MVNO (subject to approval of NTA guidelines) and accordingly offers services to its end customers.

6. M2M Sectorial Approach

i. Smart City - Creating a smart city involves making key sectors and services in the city intelligent using M2M devices - Energy, Water, Buildings, Transportation, Parking, Waste disposal, Physical safety and security, Healthcare, Education.

ii. Automotive - this includes telematics and all type of communications in vehicles, between vehicles and people/authorities, between vehicles and between vehicles and fixed locations.

iii. Power - the conventional electricity grids are undergoing a transformation with smart metering, SCADA, WAMS, substation automation etc. In addition new technologies like MW-scale grid connected batteries, micro grids, DC grids, electric vehicles etc shall change the way electric grids shall now be made/operated.

iv. Smart Water - Smart water is achieved by different types of sensors deployed across the water distribution network and across the water cycle. Intelligent electronic devices like pressure, acoustic sensors connected wirelessly allow detecting of leaks much faster. The sensors may use cellular or short range LR-WPANs/Zigbee. In case of agriculture, smart sensors help to conserve water.

v. Healthcare - Smarter healthcare management converts health related data into clinical and business insights and help provide medical services.

vi. Safety and surveillance systems - vast communication and sensor networks across cities enable law enforcement and other government agencies help ensure citizen safety and get deeper insights by analyzing the data.

vii. Agriculture - use of M2M technology in agriculture is expected to improve the productivity per hectare and lift up the sector by improved weather forecasts, soil

sensors, livestock health sensors, sensors to measure storage conditions, monitoring of insects and pests to control crop damage.

viii. Supply chain (PDS) - use of M2M solutions in food supply chain can help improve quality check and reduce pilferage. M2M can be used across various stages of PDS process - inventory management, ware house environment management, beneficiary database and authentication system, transportation & distribution.

M2M/IOT POLICY FRAMEWORK FOR NEPAL

The preparation of document is as per the Telecommunications Act 2053 sub section 23(B).

LICENSING AND SPECTRUM MANAGEMANT

Licensing and spectrum management is an important issue for ensuring availability and capacity for IoT communications. IoT devices communicate using a range of different protocols, based on their connectivity requirements and resource constraints. These include short-range radio protocols such as ZigBee, Bluetooth and Wi-Fi; mobile phone data networks; and in more specialised applications such as traffic infrastructure, longer-range radio protocols such as Ultra-Narrow Band (UNB).

Many IoT devices will be served by radio technologies that operate on unlicensed spectrum and that are designed for short-range connectivity with limited QoS and security requirements typically applicable for a home or indoor environment. Cellular technology, in combination with local connectivity technologies such as WiFi or Bluetooth, is expected to address a variety of IoT use cases providing ubiquitous mobility, resilient connectivity and economic scale.

Spectrum Requirments

There is no one, single description of the spectrum requirements for IoT services; rather, the spectrum requirements for a given IoT service will be heavily influenced by the specific nature of that service. For example,

From a technical perspective, lower frequency spectrum enables wider area coverage and better penetration deep into buildings;

From an authorisation perspective, licensed spectrum – either for private/professional networks or for public mobile networks (terrestrial systems capable of providing electronic communications services) – assures the reliable delivery of data, compared to unlicensed spectrum; and,

If there is a need for devices to have very long battery life, there may be a requirement to use bespoke and highly optimised technologies which may require their own allocation of spectrum to work efficiently.

Spectrum Requirement Considerations

In terms of spectrum requirements, provisions will have to be made within both the licence exempt frequency band and also within the licensed frequency band as,

- The bulk of the M2M market (72%) uses short-range, unlicensed connections (e.g. WiFi, Zigbee etc.)
- The wide area market is heavily reliant on cellular connectivity
    - High quality of service guarantees over wide areas, as operators are not at risk of interference and can control usage levels
- A whole portfolio of different use cases and a whole range of different needs for different type of M2M/IoT.

Spectrum Availability

M2M services is not 100% dependent on Licensed spectrum as it can operate on Unlicensed spectrum. Nepal has the unlicensed spectrum in 2.4GHz and also in the 5.8GHz bands as well as on OFC Connectivity. However, Licensed spectrum allocation for 4G-LTE and 5G (IMT-2020) does have a critical use case for critical M2M/IoT applications which demand ultra low latency and very high capacities.

The requirements of a particular IoT service will influence the technologies used to provide it, which, in turn, determine the underlying spectrum requirements. A range of existing and emerging technologies can be used to provide IoT services.

Nepal and most of the South Asia Regional countries are following the ITU-R standards for ushering in IMT-2020, which subsumes standards viz. ITU-R M.2083-0 (09/2015) & ITU-R M.2320-0(11-2014) which cater to the flexible 'network splicing' architecture to usher in 5G enabled M2M/IoT. Hence, NTA proposes that

- Spectrum allocation will be technology and service neutral.
- No separate spectrum band will be allocated exclusively for M2M services, unless it is for a very critical service or sector such as defense.
- License holders can use existing spectrum to provide IoT services.

- **M2M/IoT Service Provider(MSPs)**

M2M Services is a specialized sector based application. It needs network resources which it can obtain from a licensed TSP or an ISP. This would be in the form of data connectivity which would be required to connect to the Public Internet.

- Licensed telecom operators in Nepal will be allowed to provide M2M services in Nepal.
    - It is not mandatory for all telecom players to provide M2M/IoT services.Only those who wish to launch M2M/IoT services will register with NTA.
- NTA recognises M2M service providers(MSPs) who are not TSPs as a separate class of service providers. MSPs will be allowed to launch M2M/IoT services in Nepal. Registrationof such MSPs with NTA is mandatory.
- M2M service by itself will not be treated as a licensed service unless it is accompanied by exclusive rights viz. Licensed spectrum, Right of Way, Right

of Interconnection, Right to Numbering Plan, etc . This service inter-alia will be provided through a simple registration with NTA

- NTA may suitably amend the license conditions in respective licenses for TSPs/ISPs who wish to offer M2M services

A GSMA study indicates that over 90% of the M2M services shall work in the Unlicensed spectrum bands. World over, new technologies are being developed to provide M2M services viz. WPAN/WLAN technologies. M2M Service Providers deploying such and similar technologies like LPWAN etc. may be permitted to offer M2M services using simple registration with NTA.

- All TSP and ISP licensees interested in providing M2M/IoT services shall be permitted to offer M2M services , including in unlicensed bands,
  - NTA may suitably amend the license conditions under respective TSP and ISP categories.
- In future, if there are connectivity providers using WPAN/WLAN or other technologies for providing M2M connectivity for commercial purposes, operating in unlicensed spectrum, then they also must register with NTA.
  - NTA may charge a nominal fee to cover administrative cost.
- Connectivity provider using LPWAN or other technologies operating in unlicensed spectrum will be allowed to bid for licensed spectrum to provide exclusively M2M services, if they desire to provide M2M services in the licensed band.
- MSPs who are not TSPs have to provide to NTA, the details of the connectivity provider who would be providing connectivity to their M2M applications.

As NTA has started working to permit Mobile Virtual Network Operators (MVNO). They intend to use existing network of the MNOs (Mobile Network Operators) for the expansion of Mobile network across the country and offer new and additional services to the unserved and underserved areas. Once MVNOs are permitted in Nepal in future, then,

- All MVNO holders may be allowed to provide M2M services using licensed spectrum as an extension of the services being provided by the parent MNO.
- NTA may suitably amend the license conditions of MVNOs accordingly.

- **Regions of Operations**

Since M2M services are application and use case/need dependent, but not region/area dependent, hence region of operations may be left to the discretion/requirement/need of the M2M Service Provider. Perhaps for certain services, scale may be important and hence a pan-Nepal permission may be

relevant too. If NTA still wishesto ease operations, the circle of operations can be defined for MSPs on the basis of the regions

- Pan-Nepal
- Kathmandu Valley
- Eastern Development Region
- Eastern and Central Development Region, without Kathmandu Valley
- Western Development Region
- Mid-western Development Region and Far-western Development Region
- Provenance wise

- Government, through NTA, should identify critical services in M2Msector and these services should be mandated to be provided only by connectivity providers using licensed spectrum.
- Existing TSPs will be allowed to provide Machine-to-Machine (M2M) or IoT solutions within their specified circle of operations, if they wish to.

- **Requirement of Fresh Spectrum**

  - Requirement of additional licensed spectrum for access services to meet the projected influx of connected devices due to M2M communication needs will be assessed by NTA in consultation with all the service providers, once the momentum for adoption picks up in the country.

  - As per the global trends, most of the cellular spectrum based applications of M2M is in the narrow band or 2G (Nb-IoT) spectrum. NTA needs to assess the demand for spectrum and availability of 2G spectrum, in view of the growing demand for 4G and also for 3G.

- **SIM cards for M2M/IoT**

Since M2M is essentially a global application and would need data/traffic to flow from one country to another where expertise in Machine Learning and Big Data is available, hence, it is not practical to constrain use of only domestic SIMs for M2M purposes. Bilateral flow of data based on bilateral /multilateral agreements must be encouraged for M2M services to prosper and for citizens to benefit.

- It is not mandatory to use only domestically manufactured SIMs in M2M.
- Embedded SIMs with standard specifications comes along with imported devices like cars, health trackers, etc. NTA needs to ensure that relevant information has to be submitted by importer while import of the devices/SIMs.
- For the devices with pre-fitted embedded Universal Integrated Circuit Card (eUICC), GSMA approved guidelines shall be followed for remote provisioning with ‘Over-the-air’ (OTA) mechanism.
- Devices fitted with eUICC will have no restriction in operation, even in roaming.

- Roaming charges will not be regulated but left to bilateral negotiations between the two parties (market forces) as is the case with all ICR regulations.

- **Crtitcal Services**

  - IoT and M2M applications in healthcare, remote surgery, driverless cars etc. require high QoS, ultra reliability, very low latency, very high availability and accountability. Therefore, these critical services to be provided only by “robust wired optical fiber, copper network or LTE capable access networks.

- **Other**
  - NTA will provide broad Regulatory Framework with guidelines which would be general, non-restrictive and over-arching.
  - Sectoral guidelines would be left to the independent sectoral regulators to make within the overarching framework provided by NTA.
    - Industry regulators (apart from NTA) such as Nepal Bureau of Standards and Metrology and the Department of Drug Administration need to constitute their own regulations and policies regarding M2M and IoT solutions.

SWITCHING AND ROAMING

- **Domestic Roaming**

  - The wholesale roaming tariffs of M2M/IoT VAS services have be determined based on mutual commercial arrangements between the TSPs.

- **International Roaming**

  - This policy for machines will be based upon presently existing international roaming policy for voice and data services.
  - International roaming in M2M shall be allowed under the well-recognized framework of GSMA ‘M2M Annex’ to keep uniformity of the parameters and processes.
  - International roaming arrangements will be a matter of commercially based mutual decision between two international operators.
  - In order to boost the M2M/IoT manufacturing in Nepal, the government may consider feasibility of allowing extra-terrestrial usage of IMSI ranges

with suitable framework on the basis of country specific bilateral agreements.

- **Permanent Roaming**
    - Country specific relaxation on permanent roaming of foreign SIMs, if any, can be considered based on the strategic importance, Bilateral or Multi-lateral trade agreements and principle of reciprocity by the government.

- **Foreign SIM fitted Devices**

  Devices with pre-fitted embedded Universal Integrated Circuit Card (eUICC) will be freely allowed to be imported. GSMA approved guidelines shall be followed for remote provisioning with 'Over-the-air' (OTA) mechanism.
    - In case imported equipment to which the SIM/ device is fitted with such as automobile/ machines (like earth movers), arms etc. (requiring mandatory registration at local authorities such as the State/ District/Regional administration) is transferred/ sold to another party, then, the roaming device (eUICC) KYC details of the new owner/ buyer will be compulsorily updated in the database of concerned authorities.
    - Over-the-air (OTA) provisioning offers a preferable way to facilitate switching in the M2M space and highlights the progress that the industry has made in developing and promoting OTA capability since the first release of the GSMA embedded SIM specification.
    - With the embedded SIM or eUICC, the profile of the SIM (which includes the MNC), can be changed over-the-air after manufacture. This allows for changes to profiles of different MNOs over the life span of the product, preventing lock-in to the original MNO.
    - There is no need for any regulatory intervention for setting ceiling for roaming charges for the devices imported with in-built SIM. The market forces shall address the issue based on commercial aspects.

ADDRESSING AND NUMBERING

- NTA is optimistic about the fact that dependency on numbering system will get reduced in future as adoption of IPv6 across the networks and devices increases
- In the meantime, allocation of various network codes including Mobile network codes(MNCs) shall be to licensed TSPs only.
- There is no need to allocate MNCs or any other network codes to MSPs.

- However, in case of MSPs using unlicensed spectrum only, NTA may come up with a governance policy.

QUALITY OF SERVICE (QOS)

Different M2M applications will have different QoS requirements. Although many M2M applications have no stringent QoS requirements and can deal perfectly well with best-effort QoS, some M2M applications have higher QoS or priority requirements than normal data services. To cater to the M2M QoS needs it is important for the TSP's and MSPs to ensure good coverage along with QoS catering to Voice, Data andM2M Communications.

- Once the M2M sector develops, the Authority will put in place comprehensive regulations on QoS parameters in M2M communication, as per service requirements.
- Existing QoS benchmarks for data services will also be applicable for M2M/IoT services.
- Else, the QoS for voice services shall currently prevail.

SECURITY & PRIVACY

Security in this sector is essentially of two types' viz. data security & privacy and device security. While security by design should be embedded in all applications, software and hardware to be used, NTA or an appropriate authority will be providing an appropriate framework for

a) Data Protection, Ownership, Data Security & Privacy
b) Local Manufacturing of Devices including M2M/IoT sensors & local SIMs, etc

- "Security by design" principle needs to be implemented, and, for this, NTA along with the regulatory body for manufacturing sector needs to create fresh guidelines for manufacturing M2M/IoT devices in Nepal.
- Similarly, guidelines for importing M2M/IoT devices in Nepal needs to be created by NTA in consultation with The Nepal Bureau of Standards and Metrology (NBSM).

Standards for IoT and M2M systems: Since many M2M applications "would be operating in unlicensed bands, the government should issue specific standards for devices to be used in the M2M ecosystem, in line with international standards organizations.

- To obtain the best-in-class services, NTA would follow global standards & best practices in this field instead of devising country specific standards/guidelines.
- NTA in collaboration with NTSB will be studying international guidelines for setting up an independent IoT/M2M certification body which certifies hardware quality and will be responsible for governance and auditing of all M2M/IoT networks and devices.
- MSP shall try to incorporate in overall service design to the extent possible as under:
    i. Only point to point data, SMS and voices services to predefined numbers only shall be enabled on M2M SIM.
    ii. Enable security of Embedded Sensors to protect from computer worms, viruses or other Malware by implementation of security features like e. g. MILS (Multiple Independent Levels of SECURITY AND SAFETY).
    iii. Additional security in sensors may be incorporated by IMEI & SIM PAIR LOCKING so that sensor shall work with the SIM configured by MSP. However the reverse is not encouraged i.e. locking by TSP as it will unnecessarily bind MSP with TSP.

  These guidelines should look “the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities.” At the same time, “low-risk” IoT devices (like LED bulbs) need not be burdened with too much regulation, so the government could look at creating a “graded” level of security certification for devices.

- Managing M2M data within TSPs 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 of Nepal.
    - 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 Law Enforcement Agency shall also be applicable in case of M2M service.