The Hashemite Kingdom of Jordan
Telecommunications Regulatory Commission

Green Paper of
“Internet of Things”

TRC, Jordan
December, 2017

TRC Board Decision No. 2-17/2017 dated 31/12/2017

Table of Contents

About this paper:

This document is the first step towards the needs for developing the legal or regulatory framework for the Internet of Things (IoT), and Machine-to-Machine (M2M) communications. The document usually does not imply any commitment to action, but is a first step towards the needs for developing the legal or regulatory framework. This green paper released by the TRC, is a consultation and discussion document intended to launch the process of consultation, inviting interested telecom licensees, device suppliers, Governmental bodies and involved parties to collaborate and share views and information on this matter.

The aim of this Paper is firstly to have a clear picture of the current Jordanian market experience related to IoT services, application vendors and providers. Secondly to foresee the IoT future developments in the Jordanian communications market. And lastly, to evaluate and recommend the possible regulatory options that the TRC and the Jordanian government may adopt to tackle the challenges set by the IoT services and M2M Communications.

1. Introduction

The ITU definition of IoT is: “A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies”. [1]

This Global Concept refers to enabling large number of connected devices to communicate and share data with each other (hop to hop) - its services span industries from agriculture and energy to transport, healthcare and much more, with the potential for significant benefits to citizens and consumers.

ITU Internet Report 2005 goes on to say: " In the 2000s, we are heading into a new era of ubiquity, where the “users” of the Internet will be counted in billions and where humans may become the minority as generators and receivers of traffic. Instead, most of the traffic will flow between devices and all kinds of “things”, thereby creating a much wider and more complex Internet of Things”. The IoT holds tremendous promise for citizens, consumers, business manufacturers, network operators, application platforms, software developers and governments. Referring to devices, machines, terminals, appliances and “ things “ that are connected to the internet through multiple networks, the IoT has many means to decrease healthcare costs, increase access to education, improve transportation safety and much more. Some IoT applications may involve the wireless transmission of data over long distances, while others may operate within a single room or building. Some applications may require access to highly secure and reliable networks, while for others a lower level of security may be sufficient.[2]

The physical items, and connected sensors measuring and monitoring humans, machines and things-that are leading to a shift from human-to-human communications, to machine-to-machine communications (M2M) are factors that are setting the rapid expansion of IoT in the community , that eventually will lead to propose a clear regulatory framework.

The term Machine-to-Machine (M2M) communication is used to refer to: Communication between IoT devices that do not necessarily require human interaction.

(1) www.itu.int International Telecommunication Union

(2) www.itu.int Internet of Things Report issued on Year 2000.

In Jordan, IoT is still at an early stage in terms of implementation and regulation. For regulation, IoT issues in Jordan- as in almost the rest of the world- are currently regulated by the traditional legal and regulatory frameworks governing the Telecommunications sector, where no IoT dedicated regulation is issued. TRC is trying -by this green paper- to assess the need to develop a regulatory framework specific for IoT, and how IoT implementation challenges could be efficiently handled.

****

2. Implementing IoT and M2M Services

As the technological development evolves, and services converges, Cisco foresees that the number of devices (to provide stats) connected to the internet will exceed the number of people populating the entire planet, also the mobile industry association (GSMA) predicts between 1 and 2 billion M2M connections by year 2020.[3]

The "Things" are not just smart phones and tablets, they are sensors enabling smart grids, smarter transportation flows, tracking the health of cattle, and medical devices monitoring the health of cardiac patients.

In the Arab World, Surveillance and Security services, tracking services, Smart Home Automation, Near Field Communications (NFC) services, and IoT-related health services are offered for individuals and corporate users as IoT services.

(3) www.itu.int GSR Discussion Paper, Regulating the Internet of Things.

3. IoT implementation Challenges

There are many factors that should be taken into consideration in a serious manner when implementing IoT on a wide range. Main points are:

- **Traffic capacity**, which relates to the capability to manage a certain amount ofoffered traffic per area unit in the busy hours.
- **Mobility/coverage**, which refers to the capability to provide connectivity in anysituation; on the move and when standing still, regardless of user location.
- **Network and device energy efficiency,** which relates to the energy consumption in both wireless devices and network infrastructure. Critical factors that effects the energy efficiency are: Solution System design, energy storage development and renewable energy technology development.
- **Massive number of devices**, which relates to the capability to handle a large number of connected devices per area unit, while preventing that the related control signaling overhead limits the user experience.
- **Reliability**, which relates to the capability to provide a given service level with veryhigh probability. If reliability is high enough, mission-critical and safety-of-life applications can be supported.
- **Latency,** which refers to the time the system, needs to transport data through itsown domain of responsibility. Latency also refers to sending or receiving data within an acceptable range.
- **Spectrum and bandwidth flexibility**, which refers to the flexibility of the system design to handle different spectrum scenarios, and in particular to the capability to handle higher frequencies and wider bandwidths than today.
- **Achievable end user data rate**, which refers to the maximum data rate a user typically experiences (i.e. the “perceived speed” of the data connection).
- **The economic factor**, which determines the ability of consumers to purchase IoTsolutions including connected and enabled device: A Successful IoT implementation requires both technical and business model innovation, for example: Implementing Ipv6 and LTE .[4]
- **Interoperability and standardization**: which refers to multi-vendor device and technology coexistence.

(4)Www1.huawei.com Hawawei, IoT implementation in Japan

4. IoT and M2M regulatory, legal, Consumer rights issues

In Jordan, the telecommunication law has identified main duties and responsibilities for regulatory bodies – represented by the TRC- regarding new emerging technologies through the following statements

" *To establish the basis for regulation of the telecommunications and information technology sectors, in accordance with the established general policy, in such a way that services meet the needs of the comprehensive development in the Kingdom in accordance with instructions issued by the Board for this purpose*."

The range of legal, regulatory and rights issues associated with IoT is broad. IoT Services create new legal and policy challenges that didn't previously exist, and they amplify many challenges that already exist.

Along with the complexities of deciding the appropriate regulatory framework for IoT challenges, there is the added complexity of deciding where in an IoT system architecture is the best approach to achieve the optimal desired outcomes.

Moreover, should the regulatory controls be implemented against devices, allocated spectrum, data flow, the gateways, user rights, or where data is stored?

The answers to such questions and others depend on the perspective taken to analyze the situation. Regulatory analysis of IoT devices is increasingly viewed from a general, technology-neutral perspective legal lens, such as consumer protection laws and regulations.

Assessing legal implications of IoT devices from the perspective of preventing unfair or deceptive practices against consumers can help inform decision makers regarding privacy and security among others.

From another point, IoT can help make society more effective, safer and greener so it is important to take into account that the future regulations strike a proper balance between supporting helpful innovation and protecting consumers. It is also important that these future regulations to be in accordance with international approaches and experiences.

In this context, the main IoT regulatory, legal issues are:

I. Spectrum management and Licensing for connectivity

IoT services may be deployed using a range of communication technologies, both wired and wireless. However, many of these services will require the flexibility or mobility of wireless networks and will, therefore, rely on the availability of spectrum to support their connectivity.

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.

Currently TRC do not consider spectrum availability to be a barrier to the development of the IoT/M2M in the short to medium term. The low data rates typical of the majority of emerging IoT/M2M applications mean that they can be supported within existing allocations. We have also taken steps to study additional spectrum available for IoT/M2M services, such as the millimeter-wave frequencies bands, and are examining the possibility of making spectrum in these bands available. Many IoT/M2M applications that require short-range wireless connectivity could also use spectrum at 2.4 and 5GHz, which is used by a range of services and technologies including Wi-Fi.

However, the spectrum requirements for the IoT in the longer term are uncertain; the market is currently immature and future generations of IoT applications might have increased demands for spectrum. It will be important, therefore, to continue to monitor the development of the IoT to help anticipate and prepare for any significant changes in spectrum demand.

Spectrum is available for a wide range of IoT application in different bands and there are no spectrum bottlenecks for dedicated IoT systems yet . As of now, most IoT systems operate in unlicensed radio frequencies, namely in the ISM (industrial, scientific, and medical) bands at low bandwidth using a range of different (and sometimes competing) wireless connectivity standards, such as Bluetooth, ZigBee, Z-Wave, and Wi-Fi (802.11 Standards) , all of which were designed to work in ISM -unlicensed internationally- spectrum bands such as using wirelessly connected sensors for smart farming; intelligent traffic management systems; and smart energy: video surveillance and access control systems; near-field communications (NFC/ ISO/IEC 14443 and ISO/IEC 18000-3) for mobile payments; and Electronic Product Code (EPC) and Radio Frequency Identification (RFID) usage.

On the other hand, Licensed spectrum available with the MNO's as on date as well as the spectrum likely to be made available in the near future (mid –term) is sufficient to meet spectrum requirements for IoT and M2M. Mobile Networks support a wide area M2M of today's market for low bandwidth applications, such as vending machines, and through 3G and 4G-LTE for high bandwidth applications such as streaming video. MN's also support LPWA IoT applications(3GPP- low power wide area) in almost all licensed mobile bands including the ability to support personal and IoT connectivity in the same frequency band at the same time.

The international harmonization of spectrum and standards is also likely to be vital for delivering economies of scale and lower cost subscriber equipment; given the need for very low cost equipment for certain applications, this will be particularly important for the longer term success of the IoT.

Radio Technologies

Most IoT applications will be supported by radio spectrum technology standards in the ISM bands and those of licensed radio mobile networks (MNs).

ISM spectrum technology standards such as :

- Bluetooth (IEEE 802.15.1/ Bluetooth SIG in the 2.4 GHz band) for distance Ranges of 50-150m and Data Rates around 1Mbps

EXAMPLES of IoT applications through Bluetooth connectivity: Audio and mobile applications Sports and fitness accessories (‘wearables’)

Wi-Fi IEEE 802.11 standard (in both 2.4-GHz & 5-GHz ISM bands) for distance Ranges of Range: Approximately 50m and Data Rates: 150-600 Mbps maximum (depending on channel frequency used and number of antennas0

EXAMPLES of IoT applications through WLAN connectivity: Smart home thermostats/power meters Smart city technology such as parking meters

ZigBee IEEE802.15.4 in the 2.4 GHz band for distance Ranges of 10-100m and Data Rates around 250kbps

EXAMPLES of IoT applications through ZigBee is Remote Control

Lower-Power Wide Area Networks (LPWAN) at a low-bit rate for devices

EXAMPLES of IoT applications through LPWAN connectivity: Remote monitoring systems Remote alarm systems, Smart agriculture, Sensor networks, battery operated sensors.

NFC (Near Field Communication) ISO/IEC 18000-3 in 13.56MHz (ISM) band for distance Range: 10cm and Data Rates: 100–420kbps

EXAMPLES of IoT applications through NFC is a two-way interactions between electronic devices: such as allowing customer to perform contactless payment transactions (via smartphones), access digital content and connect electronic devices.

Licensed mobile Networks (application that requires operation over longer distances)

EXAMPLES of IoT applications through licensed mobile network connectivity: Logistics - asset tracking for fleet management, Transport - smart car technology and keyless locking systems

Utilizing existing networks helps to retain some of the key advantages of cellular systems including strong security, excellent coverage, and roaming capabilities, and assured quality of service (QoS) by operating in a licensed spectrum.

Recent changes in 3GPP standards are beneficial for IoT applications. Mass improvements have been made to increase power savings and extend battery life. Connectivity capabilities have also improved greatly. Connectivity is now capable of extending into subterranean locations and penetrating walls and floors.

Mobile Operators must monitor availability for short and long range IoT communications and their backhaul network capacity also they have to encourage next generation technology and small-cell technology using IMT technologies have the ability to enhance capacity and per-user throughput, as well as reducing costs and uniquely offering tight cooperation with the macro coverage layer.

Small cells using low power nodes are considered promising to cope with the expected mobile traffic demands, especially for hotspot deployments in indoor and outdoor scenarios. They are often employed by mobile network operators to extend the reach and quality of their networks.

Small cells, which can include femtocells, picocells and microcells, provide a small radio footprint ranging from 10 meters within urban areas to 2 km in rural locations. Mobile operators often use small cells to extend their service coverage or to increase network capacity in areas of high demand.

They may have an important role to play in enabling IMT-2020, which many expect to rely on heterogeneous networks (discussed below) of different cell sizes to provide more ubiquitous connectivity. Providing backhaul to these small cells can be challenging since they are often in hard to reach places and require carrier grade connectivity.

i.1 Millimeter-wave:

Millimeter wave (also millimeter band) is the band of spectrum between 30 gigahertz (GHz) and 300 GHz. 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.

The frequency and throughput are proportional to each other. Higher throughput is achieved when the frequency is higher. The mmW frequency bands such as (V&E-bands) can handle data rates into a multi-Gbps ranges.. The mmW bands do not go long distances, but can be used in a radius for faster speeds ,they act as a "fiber extension" to extend broadband connectivity for the applications.

The mmWave makes possible the use of large numbers of antennas in a multiple-in multiple-out (MIMO) configuration. Arrays of antennas , connected to low-power amplifiers in the milli-Watt range can simultaneously connect to tens of terminals. The result of these technology advances is high spectrum efficiency and overall capacity will be increased by a factor of around 10 times over the use of a single Antenna, thus opening the domain for 5G wireless broadband technology on millimeter wave spectruma and expanding IoT applications, since they are capable of carrying higher bandwidth applications.

i.2 Meeting future demand for spectrum:

Modifying the usage conditions for specific bands for new use and users on a licensed or licence exempt basis; - Opening up bands for access on a shared basis.
Modifying licence obligations to allow the deployment of IoT-optimised technologies within their existing spectrum allocation.

i.3 Radio Coverage in Buildings:

Different frequencies penetrate buildings and structure in a manner that signal loss will occur, and since building structures are made up of different materials that either absorb Radio frequency, or reflect it, ways to improve Radio coverage in Buildings is needed, and at this point First Window coverage will be required especially for residential buildings that are not usually equipped with boosters or amplifier systems, while commercial buildings can have many solutions for radio coverage improvement such as Distributed Antenna Systems (DAS) that is a network of radio frequency cables or fiber optic cables with antenna terminations throughout a building or structure, or Bi-Directional Amplifier that rebroadcasts RF signals..

ii. Switching and Roaming

Once the IoT is widely offered, development of SIMs and mobile network accounts suitable for large M2M users, roaming mobile devices, and fixed devices in areas of poor mobile coverage is needed.

From a regulator’s perspective, there are typical roaming scenarios in IoT connected devices that can be described: 7

1. Connected IoT device is moving or traveling periodically, within local domestic network such as a connected vehicle. In this scenario there is no permanent roaming applicable, which leads to no necessary regulating steps, since there will be no extra costs upon using the service through the same network.
2. Connected IoT object is located within domestic or permanent roaming boundaries most of the time, but it might travel within the country or to a neighbor country across borders.
3. The connected device is not traveling at all, and it is used on the basis of permanent roaming most of the time. In this scenario, no certain regulatory steps are needed.

Switching connectivity service provider requires a hardware modification of the IoT device (such as the replacement of the connectivity module or, the replacement of the SIM card), but the cost of dispatching technicians for each IoT device might be critical, especially for extensive deployments of equipment. As a result, it could negatively impact the incentives for an IoT user to switch to another connectivity service provider.

In addition, the switching cost could be important for a competitive IoT environment and the users should carefully know the pros and cons (maybe in contract) of the offered connectivity technologies by IoT service providers, because switching connectivity service provider may in many cases require switching the connectivity technology and replacing the related hardware.

There is a believe that the ease of switching between connectivity service providers as well as IoT service providers is important in order to create a competitive environment for IoT services.

(7) www.berec.europa.eu/ Body of European Regulators

iii. Competition

Reports finds an optimistic picture for the IoT/M2M industry. It is expected that in the near future , this market will reach billions with respect to terminals and revenues,
however, operators cannot stand still as increasing competition aims to take advantage of the growing demand for M2M/IoT, Growing cellular systems, and the rollout of 5G networks, will increase competition within the M2M/IoT market globally.

Changes in technology clearly require changes in business models. The IoT will certainly drive the development of new business models in the telecom market.

Applying competition practices is needed to avoid IoT user lock-in and new barriers to entry the IoT market.

iv. Security

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 attackers 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 :

1. Efficient Encryption algorithms running IoT devices and networks need higher processing power. (Low CPU power vs effective encryption).
2. 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.
3. Crypto algorithms have a limited lifetime before they are broken, which may outlive the original running application. (ex: smart metering systems may last 40 years).
4. Authenticating to multiple networks securely.
5. Data availability to multiple collectors synchronously and securely.

[2] www.cisco.comCISCONetworks , Securing the Internet of Things, Proposing a framework

1. 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.
2. 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, andsensoring equipment.

As the number of “Things” start 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: 9

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 unautharized 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.

(9) www.Inttechservices.com

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, MoICT Jordan produce a public consultation on "Personal Data Protection Law" and expected to be finalized for approval in 2017 .

Addressing and Numbering

To realize the Internet of Things services and increase it's spread; the existing information and communication technologies should evolve to support the characteristics of the IoT and the most enabler for that increasing is the Addressing and numbering. So, a Large address space needed for globally addressable things (although many IoT devices only need local connectivity). Deployment of IPv6 by ISPs, public and private sector organizations is the key to have this large number of needed addresses. Use of IMSI (The International Mobile Subscriber Identity) is also required to address devices at some certain IoT services, and especially when the IoT services in the M2M communication use IMSI extraterritorial.[10]

IPv6 is the future scheme of the internet-addressing scheme which can provide each individual person on earth with more than 40 billion objects, and each address is coded using 128 bits as opposed to 32 bits as with the existing internet protocol (IPv4).

[10] www.itu.int International Telecommunication Union, Requirements and Common Characteristics of the IoT Identifier for the IoT service.

5. Conclusion and recommendations

TRC has identified several priority areas to help support the growth of the IoT/M2M. Following feedback from the sector in April ,2017, these areas include licensing, spectrum availability, data privacy and network security , numbering and addresses, competition , roaming and switching and standardization and communication technologies.

In this section we set out our conclusions and proposed next steps, grouped into the key areas, based on responses to the first draft of this paper (April 26th 2017)   and our own analysis. Some of these areas are a good fit with TRCs existing regulations, while for others there is the potential for TRC to facilitate the provision of IoT/M2M services.

First - Licensing

TRC believes that current existing Licensing Regime is capable of adopting new technologies such as IoT/M2M since it is a technology neutrality regime and thus any one can apply to this existing licensing regime. In the meantime TRC will keep Encouraging investment of new technologies networks (weather wired or wireless) , and revisit the requirement of additional spectrum for access services to meet the connected devices spectrum requirements due to M2M and IoT. TRC will also make all resources available to provide information and help for those seeking the provision of IoT/M2M.

I. Any request can be handled depending to its nature and type of service (mobile or fixed) according to the following options:

1. Existing Mobile networks (2G , 3G ,4G and beyond):
   a. Type I: by the existing licensee who has a license to provide public mobile telecommunications services (individual). In such case only a Spectrum License is required if a new of additional frequency is needed to provide the service.
   b. Type II: Using existing infrastructure of the licensed mobile telecommunications operator MNO by the provider. In this case the MNO licensee should comply with all license conditions and of the TRC instructions and be responsible for all the requirements related to the provision of the services

2- Type III : request the use of new frequencies for the provision of the (IoT/M2M) service only . A public telecommunication (Individual) license and general spectrum license are required.

3- Type IV: Provision of service on secondary basis frequencies such as ISM bands, low-power devices (SRD short range devices), as approved by TRC In such case a public telecommunications license (Class) is required; and the conditions and requirements of the license must met. If the technical requirements of the technology to which the service is provided exceed what is approved by the TRC such as the radio equipment exceeds the adopted low power by TRC for the equipment in such case an individual license and spectrum license are required.

4- Type V : Providing the service by the operator/applicant for own and private use . In such case the operator/applicant must abide to the instructions of the private networks and no need for any license to provide the service except in the case of requesting frequencies where frequencies are granted according to the exciting spectrum policies and instructions.

II. Fees

TRC's current charges and licensing fees according to the nature and type of license, in particular frequency charges and annual spectrum licensing fees and revenue share

Second -Spectrum

TRC understand that the IoT/M2M market is not mature yet , but as a regulator will ensure accommodating any application and the availability of all resources for the applications in the needed time including spectrum .

TRC will continue to adhere to its policy in allocating Spectrum in a technology neutrality basis - No separate spectrum band should be allocated exclusively for IoT/M2M services-. In the same time TRC will also keep allocating and licensing of Harmonized (regionally and globally) radio spectrum Services bands to support all IoT use cases for LPWA and for high bandwidth applications, in order to reduce the cost of terminals and therefore accelerate adoption of radio services including those of IoT. Suitable existing bands include the 900/1800MHz bands and the700/800/ 850/1900MHz bands which have globally harmonized for mobile radio services and of reach for IoT especially if technologies allow IoT applications in the guard bands. In case it should be noted that critical IoT/M2M services should be provided under licensed spectrum: TRC will study which critical Services should

Identify and differentiate them from non-critical services. For example IoT and M2M applications in healthcare, remote surgery etc. require high QoS, ultra reliability, very low latency, very high availability and accountability. Therefore, these critical services should be provided only though licensed Spectrum and networks.

In the meantime anyone can apply for our existing Spectrum License Regime. Taking into consideration that TRC will keep Encouraging investment of new technologies networks (weather wired or wireless) , and revisit the Requirement of additional licensed spectrum for access services to meet the connected devices spectrum requirements due to M2M and IoT. TRC will also make all resource available to provide information and help for those seeking to use spectrum for IoT/M2M.

Frequency bands that can be used in IoT services fall under the following categories/cases:

1. Frequencies that do not require an "individual license', which are allocated on a secondary basis, namely ISM Bands or so-called (Unlicensed or shared bands) as TRC allows the use of frequencies on a secondary basis for low power or SRD radio communications equipment . In this regards TRC will consider for IoT only those frequency bands that are internationally harmonized used on sharing basis or ISM bands such as those for WiFi, Bluetooth, Zigbee, which are considered under IEEE 802.11 or near-field communications (NFC / ISO / IEC 14443 and ISO / IEC 18000-3) Electronic Product Code) and Radio Frequency Identification (RFID) usage or those for satellite VSAT frequencies that do not require international coordination to protect them against harmful interference .

<u>In this case only a Public Class License is required</u>

2. Frequencies that requires an "individual license, which are allocated on a primary basis and are protected from interference to mobile, fixed or satellite services such as: - 2G, 3G, 4G and 5G) and their related IoT/M2M systems like EC-GSM-IoT(Extended coverage GSM for IoT) or enhancement to EGPRS for M2M or LTE-eMTC (, LTE evolution for massive MTC (3GPP Release 13)) or NB-IoT over LTE (3GPP-LPWA), - terrestrial services frequencies in general (fixed or mobile) within the IEEE 802.16 standard such as WiMAX or wireless local loop, - other mobile terrestrial services such as (PMR: Professional mobile radio networks) - Frequencies of satellite services that requires coordination such as mobile or fixed-axis satellite communications systems

In this case Individual License and General Spectrum License are required

3. Examples of internationally frequency bands which are under study to be allocated on harmonization basis are the following frequency bands (Not binding to TRC):,

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	

4.Radio technologies

TRC understands that in all cases standardization of technologies (and harmonization of frequency bands) is required for interoperability and compatibility reasons. However, TRC will consider technology neutrality as no single standard will be able to cover all IoT/M2M cases due to the enormous variety of applications.

5.Backhauling

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 TRC will consider if new frequency bands might needed for backhaul applications and channel plans that could support the use of broadband radio systems

In the meantime TRC will encourage all efficient and flexible wireless technologies, (as well as the wired technologies especially the optic fiber) including point-to-multipoint (PMP), adaptive modulation and antenna technology, Het net …etc ., in order to accommodate the requirements and demands of backhaul for the different radio services.

Third- Numbering and addressing

1- Numbering

TRC considers that there is still a role for the use of a national number ranges for extra M2M/IoT applications. However, numbers will be assigned - if necessary - in accordance with the national numbering plan and as approved by the International Telecommunication Union (ITU) and what will be adopted in the future for IoT services, in particular:

- ITU-T E.164 - ITU-T E 164. (International / global E.164 numbers), ITU-T E.212 IMSI (MNCs under MCC At network level 9)
- If the operator's network is used for mobile services, the operator's numbers are used and no special numbers are assigned to the service provider.

NOTE: TRC issued a consultation to update it's a national numbering plan and proposed a new digital range for IoT services.

2- Addressing

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 128Ibit addresses. TRC encourages and prefers 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.

Fourth- Security and Privacy

1- Security

Globally it is appeared that IoT providers should implement reasonable security actions. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities.

TRC will conduct intensive studies in order to issue strong, flexible, and technology-neutral regulations and recommend reasonable and appropriate security practices for the operators to strengthen the data security

In the meantime as this subject is still quite immature TRC encourages the operators to consider more security and privacy issues to notify subscribers when there is a security breach ,and to adopt reasonable and appropriate security practices to address data breaches and protecting subscribers from outside threats. In this regards TRC encourages the operators to consider the following:

1-operators should establish and build security and privacy systems in their networks and to ensure the availability and compatibility of the equipment with them before launching of the service as a key part in the design process of the network and provide it to the TRC in advance prior the provision of the service. The operators should take the following actions:

(1) Conduct a security risk assessment; and (2) test their security measures before launching their service.

2- Operators should train their employees about good security, and ensure that security issues are addressed at the appropriate level of responsibility within the company.

3- Operators should retain only service providers that are capable of maintaining reasonable security and provide reasonable oversight for these service providers.

4- Operators should implement a defense approach, in which they consider implementing security measures at different several levels in the cases that they identify significant risks within their systems.

5- Operators should consider implementing reasonable access control measures to limit the ability of an unauthorized access to the subscriber's device, data, or even the network.

6-Operators should continue to monitor their systems and the devices throughout the life cycle and in continuous bases develop a feasible protection patches and detect any gaps in them network . They should also communicate with manufacturers and software developers to update and to improve the encryption and security systems or change those devices and software if they can not comply with the Safety and privacy requirements.

7- Operators should determine the basis for dealing with information and data that is classified as sensitive information / data and provide technical information to the TRC that demonstrates how they treated it as a highly sensitive information / data.

8- Operators shall submit periodic reports to TRC and other concerned governmental authorities on the breaches made on their network and the subscriber's equipment used in the service, any technical gaps that arise and how to deal with them, and how they are going to improve safety and privacy matters.

9- Operators should participate in the committees formed by the TRC with the concerned government entities to follow up the security and privacy issues on the networks and services they provide, such committee will held their meetings periodically where operators provide the committee with all necessary information and abide to the technical bases agreed upon in the committees to deal with any gaps or breaches of privacy and network security.

10- The service provider will be obliged to disclose to the subscriber information on how to deal with personal data how to maintain it through a clear and special publication for this purpose.

2- Privacy: In so far as the IoT involves the collection and use of information identifying individuals, it will be treated by Jordanian legislation such as the Data Protection Law. TRC believes that a common framework that allows subscribers easily and transparently to authorize the conditions under which data collected by their devices is used and shared by others will be critical to future development of the IoT sector. Given this, TRC will explore how it can support and work with the Government entities and the industry to facilitate progress on this issue in the national level. However and since privacy is a big issue with IoT, TRC will emphasize the necessity of all data must be encrypted.

Fifth- Standardization and communication techniques

1- Standardization: The equipment used should be:

- Certified by international recognized standardization institutes accredited in their countries
- Interoperable and not proprietary standards
- Open Standards : open standard characteristic reduces the risk of technology becoming redundant. It also helps to ensure that users of the technology are not “locked-in” to a specific vendor or operator.

2- Communications Technologies

TRC understands that in all cases standardization of technologies (and harmonization of frequency bands) is required for interoperability and compatibility reasons. However, TRC will consider technology neutrality as no single standard will be able to cover all IoT/M2M cases due to the enormous variety of applications, i.e communication technologies shall be interoperable harmonized and of those internationally recognized and certified by international standardization bodies such as IEEE, 3GPP or 5G PPP, Radio technologies

Sixth - Competition

TRC will encourages and foster investment for new globally interoperable IOT/M2M technologies and keep under review whether ex post investigations of abuse of dominant positions will be sufficient to foster a competitive market and rapid innovation.

Seventh – Roaming

TRC believes that Roaming for IoT/M2M Service Providers and MNOs have several benefits:

- Roaming gives mobile or stationary devices the advantage for multi-national deployments with no local connection needed,
- It minimizes the number of providers needed for connectivity
- It provides a potentially multi-MNO environment for a seamless guaranteed coverage.

But, MNOs will also face a number of challenges coming from the scale of deployment which may not be easily resolved among themselves and with international standards supporting them. Therefore, TRC will keep studying the best international regulatory actions (where necessary) that will not affect national security for IoT/M2M roaming and work towards solutions to help the MNO's , in specific:

- Support – where necessary - MNO's face IoT Roaming challenges and allow them to benefit from optimal pricing.

- Support IoT Roaming transparency and the resilience of best coverage.

- Prepare and plan to provide tools that will facilitate MNo's adaptation to this changing technological environment.

- Cooperate with the MNO's to find the best ways they should adapt the roaming rates based on the new behavior of devices or "things" with SIMs when they are roaming
- Facilitate – when needed- roaming scenarios for M2M/IoT services at fair and equitable conditions for all the parties involved.
- Allow – where applicable- the use of national numbering resources through roaming to make M2M/IoT services viable.
- Adopt - if necessary- policies that recognize and facilitate cross border data flows and permanent M2M/IoT roaming in line with international best practices

Moreover, in most cases, without roaming M2M applications simply may not be viable. Therefore, in order to facilitate the growth and development of M2M services, TRC will encourage the MNo's to establish a bilateral commercial roaming models used between mobile operators that provide a practical basis for accommodating and facilitating M2M service,.

END