The Hashemite Kingdom of Jordan
Telecommunications Regulatory Commission

Green Paper of "Internet of Things"

Issued on April 26th 2017

TRC, Jordan
April, 2017

Table of Contents

About this green paper:

This Green Paper 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 Green 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 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 directly between IoT devices without the need of human interaction, often via cellular networks, WiFi, Bluetooth and RFID.

(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.

Please Answer:

1: Is the definition of IoT mentioned previously complying with your vision and the services you provide . If not, please elaborate

****

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.

Please Answer:

2.1: Do you offer any IoT services in the Jordanian market? If Yes, answer the following:

2.1.2: Kindly, list and briefly explain those services.

If your answer is no, please answer the below question:

2.2: Do you have future plans to offer new IoT services in Jordan? What services? And timeframe? Please elaborate. **

(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 of offered traffic per area unit in the busy hours.
- **Mobility/coverage,** which refers to the capability to provide connectivity in any situation; 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 very high 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 its own 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 IoT solutions 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

➢ *Please Answer:*

3.1: What are your expectations to the IoT traffic capacity in Jordan for the next 5 years?

3.2: In which fields of implementation it's expected to have the highest "data interaction" traffic and which is expected to be the lowest?

3.3: Please arrange the above mentioned challenges in terms of limiting the IoT wide implementation, from the most affecting factor to the least. Please justify and elaborate.

3.4: Are the data rates offered in Jordan sufficient to handle the IoT traffic especially for time - sensitive services?

3.5 : Please suggest at least three categories that classify the services that reflects reliablity levels that can be needed.

3.6 Please classify the services in term of latency acceptance ranges.

3.7 Please list any further challenges that might affect the implementation.

****

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

In Jordan, the telecommunication law has identified main duties and responsabilities for regulatory bodies – represented by the TRC- regarding new emerging technolgies 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.

Please Answer:

4.1: Do you think that at the current stage of time there should be a specific regulation for IoT and M2M?

4.1.1: If yes, what are the suggested topics that should be covered in the IoT regulation? If No,

4.1.2: From your point of view:

- What is the possible solution for handling the IoT issues at the current stage?

- Do you think that TRC should deal with the impacts of IoT services on security , privacy, numbering, spectrum and competition and be ready if companies chose to provide them at large? Or not doing anything until these issues become mature and regulated globally?

4.2: How can you solve the above mentioned challenges that face the consumers?

4.3: What indicators and when do you think is the right time to regulate IoT?

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 managment 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,WiFi and Mobile networks ,and in more specialised applications such as traffic insfrastructure longer range radio protocols such as Ultra-Narrow Band (UNB).

Because wireless connectivity is a very important issue of enabling IoT services, ensuring that spectrum is available for a wide range of IoT applications, at short and long ranges, in licensed (3GPP : 2G , 3G , 4G and 5G) and unlicensed (Non-3GPP : Wifi and Wimax) bands is highly needed.

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 (ECS) 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.[5]

(5) ECS stands for electronic communications services, provided by means of electronic signals over, for example, telecommunications or broadcasting networks. ITU.

Personal and local area technologies: Short range connectivity can be provided by conventional, general purpose technologies such as Wi-Fi or Bluetooth. These technologies may be particularly appropriate for consumer IoT services, such as health or fitness trackers. Optimised versions of Bluetooth and Wi-Fi are also emerging; - Wide area low power technologies: A number of bespoke technologies are being developed and are optimised specifically for certain IoT services.

On the other hand, for what regarding Mobile technologies, existing mobile networks, such as GSM, UMTS, and LTE have been used for several years to provide wireless point of sale applications. Various technical enhancements are being proposed which will enable mobile networks to support a wider range of IoT services more efficiently and allowing connectivity service providers to support these services using much of their existing infrastructure. These enhancements include an air interface capable of efficiently supporting IoT services within a 200 KHz channel bandwidth called NB-IoT and IoT-optimised variants of the LTE standard used for 4G services. In the longer term, 5G networks will emerge that will efficiently support a range of services, including IoT; and - Satellite technology. [6]

WiFi provides a highly affordable and scalably way to offloading form mobile networks for the huge traffic coming from IoT devices.

Mobile Operators must mointer availability for short and long range IoT communications and thier 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.

(6) NarrowBand IoT (NB-IoT) is a Low Power Wide Area Network (LPWAN) radio technology standard that has been developed to enable a wide range of devices and services to be connected using cellular telecommunications bands.

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:

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 recent World Radio communication Conference 2015 (WRC-15) debated bands to study for IMT for 2020 and beyond. It decided to consider the following bands, many of which are millimeter-wave bands: 24.25-27.5 GHz, 31.8-33.4 GHz, 37-40.5 GHz, 40.5-42.5 GHz, 42.5-43.5 GHz, 45.5-47 GHz, 47-47.2 GHz, 47.2- 50.2 GHz, 50.4-52.6 GHz, 66-76 GHz and 81-86 GHz. Since several other services use portions of these bands (e.g. fixed, radiolocation, radionavigation and different satellite services) and considering that parts of those bands do not have a global mobile allocation, the ITU-R will undertake compatibility studies to determine the feasibility of using these bands for /IMT,IMT-2020 (5G), for consideration and adoption by WRC-19.

Evaluate spectrum resources to satisfy IoT needs, both current and future.

Different elements of the IoT, from machines to sensors, need a variety of spectrum resources that is fit for purpose, relevant authorities should assess future demands for spectrum and review the mechanisms by which spectrum could be made available for range of uses, including for IoT.

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. Most Recommended frequency is 700 MHz which penetrates inside deep doors.

Please Answer:

4.4 Do you think at the current stage of time an intervention by TRC should be taken to regulate Licensing and spectrum management to enable/allow providing IoT service in the kingdom through allocating spectrum for IoT Services?

If Yes, how this can be achieved? Please elaborate. If no,

4.5 When the review should take place to specify the need of taking an action?

4.6 If you offering or planning to offer IoT services in the Jordanian market, Please list what type of connectivity methods and technologies you are using (or will use)?

4.7 Do you think that the spectrum and backhaul capacity you have will meet the demand of the IoT needs?

4.8 Regarding the millimeter wave bands, do you think they will be useful and meet the requirements of IoT?

****

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 romaing scenarious 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 permamnet 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

➢ *Please Answer:*

4.6 When do you think such development of mobile networks as mentioned previously *(in section ii switching and roaming)* will be needed in Jordan?

4.7 Is there any need for a regulatory framework by the TRC to regulate the IoT roaming issues?

4.8 Do you think that the current signed roaming agreements are appropriate to encourage IoT services in Jordan? Or do those agreements need update?

4.9 Is your company welling to dedicate SIMs for M2M Communications? if Yes , will the cost rates vary from normal roaming services?

4.10 Is there any need to draw a distinction between person-to-person communications and IoT connected devices in terms of roaming?

4.11 Is there any need for the TRC to intervene in switching process, mechanisms, switching mechanisms, and cost for the purpose of achieving a competitive market for IoT services? If not, more explanation is needed.

****

iii. Competition

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.

Please Answer:

4.8 When do you think that regulating market competition issue of IoT in Jordan will be a critical issue?

4.9 Are the competition regulations in Jordan sufficient to handle the above IoT issue? Or a modification on the current regulations is needed? Or a new separate regulation for the competition in IoT issues should be adopted? Please elaborate on more details.

4.10 Is there a need for issuing market structures and pricing schemes that defines IoT services pricing and describing how IoT can drive competitive advantage through better information and more localized decision making? Please elaborate

****

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 managment 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 :[8]

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 communucations 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. .
6. 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 .
7. The attack surface is dramtecally increased ,an extensive leverage of open networks will be exposed .

(8) www.cisco.com CISCO Networks , Securing the Internet of Things, Proposing a framework

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" 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 comprehansive 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

Please Answer:

If you provide an IoT services,

4.11 Do you have a policy for visibility and secure management of "Things" on your network today?

4.12 Are you collecting management or visibility information from the "Things" on your network?

4.13 How are you collecting security and operations data about "Things" on your network?

4.14 How would you rate your ability to provide security to the "IoT" services?

4.15 What controls do you plan on deploying in the next 5 years to protect against security risks?

4.16 What do you think the greatest security threat to the IoT will be over the next 5 years?

Regardless if you do or not providing IoT services, please answer the following:

4.17 Who should take responsibility for managing the risk imposed by new "Things" connecting to the Internet and the local network? And when is the best time that to issue a regulation to protect security?

4.18 Do you think that there is a need for security protection regulation to be issued in the current time?

If No, when is the best time that a regulation to protect security should be issued?

4.19 Do you think that securing IoT will demand to restructure your current organization's security policies and directives? If yes please explain how. If No, how you are planning to handle IoT services and devices security?

4.20 Are you dedicating Gateways, IPS, and Network monitoring systems to your connected "Things"? Or you are utilizing your current Network infrastructure and systems?

4.21 What kind of encryption algorithms your organization uses for your network 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, MoICT Jordan produce a public consultation on "Personal Data Protection Law" and expected to be finalized for approval in 2017 .

➢ *Please Answer:*

If you provide an IoT services,

4.19 Do you have a policy for data privacy and protection of "IoT" services today? If yes, how do you apply this policy? And do your consumers aware of such policies?

4.20 How would you rate your ability to protect privacy of the "IoT" data?

4.21 What controls do you plan on deploying in the next 5 years to protect data privacy?

4.22 Do you think that there is a need for data privacy protection regulation specific for IoT services to be issued?

4.23 From your point of view, do you think customers and end users should have any assurance of privacy when subscribing to IoT services? If yes, please mention how should this be achieved? If No, please elaborate.

****

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).

Please Answer:

4.23 IF you are providing IoT services, what do you are using to differentiate the numbers used for IoT services-Is there any specific numbers or ranges for IoT services- please List it if any?

4.24 Do you think that there is a need for specifying a numbering range (in the National Numbering Plan) for IoT services in the current time?

If yes, Please suggest a numbering range for IoT services.

4.25 Do you think that the late migration to IPv6 will limit the IoT expansion?

4.26 Do you agree to use a specific code (MCC) in IMSIs permanently for M2M services abroad?

4.27 In case MVNO, what are your arrangements to enable them to use your Network to provide the IoT services to their customer inside the Kingdom And outside?

4.28 What is the percentage of Internet addresses using version six that are used to provide IoT services to those using version four in your network?

4.29 List and Clarify the percentage of the IoT services interim their identifiers that used by your network (IP address, MAC address ...) to provide IoT services?

4.30 Any recommendation about the Addressing and Numbering for IoT services provided by non-telecommunication licensed companies?

****

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

5. Conclusion and recommendations

TRC anticipates that the near future will widely embrace the implementation of the IoT services in the Kingdom matching the rapid evolving technology needs in the Globe, such services that may include many applications within many sectors and it will affect a lot of parties that benefits from these services in many sectors, for example of that sectors but not limited to : health, agriculture, Energy consumption, manufacturing, vehicles tracking and maintenance, smart home, and surveillance systems.

Therefore, TRC in order to assess the need at current stage to develop a regulatory framework specific for IoT, and how IoT implementation challenges could be efficiently handled; conveys the following recommendations:

1. Start with identifying a realistic and reasonable "status quo" of IoT in Jordan, such approach will be necessary to envision the next step, and can be visualized by submitting realistic answers of the questions contained through this green paper to the telecom licensees and interested entities.
2. It is important to be ready for a proof of concept regarding a next step towards a regulatory framework regarding IoT, cloud computing and Big Data in advance, being ready at the early stages, before competition, privacy and security become more complex issues to handle.
3. Raising any further issues might be related to enabling and encouraging the IoT services in the Jordanian market, so therefore your feedback and comments in this regard are much appreciated, and can be delivered as an attachment to your answers.
4. Upon the received feedback from the consultation, TRC might invite any entity to present the specifications of IoT services they provide to beneficiaries. Such step can help TRC to identify any issue that can be raised later.

END