Petra Jordanian Mobile Telecommunications Company (Orange Mobile) comments to the Green Paper of Internet of Things

Orange Mobile welcomes the opportunity to participate in this consultation and shares its views on this important matter with the TRC, and hope that our comments are taken into consideration.

Orange Mobile comments are structures into two parts; (A) General comments, and (B) Specific comments.

A. General comments:

As rapid development of a variety of services that make use of Internet of Things (IoT) and Machine-to-Machine (M2M) communication has recently taken place, Orange Mobile supports the TRC efforts to have a clear picture of the current Jordanian market experience related to IoT; to foresee the IoT future developments in the Jordanian communications market and to evaluate the possible regulatory options that the TRC and the Jordanian government may adopt to tackle the challenges and unlock the socio-economic benefits of IoT and M2M communications.

The improvement in the infrastructural environment around IoT/M2M has led to a rapid growth of applications and services that meet users' business and lifestyle needs. M2M/IoT technologies are being used in a wide range of so-called "vertical industries", including transport, smart homes and cities, energy, payments and e-health.

The IoT and M2M market is characterized by partnerships between different players in the value chain – and as such is a complex market with cross-industry partnerships (involving hardware providers, device suppliers, application developers, communication service providers and systems integrators) which enable the market to meet the differing requirements of the businesses that are now integrating IoT and M2M technology within their everyday operations.

Therefore, we strongly believe that a national IoT strategy or plan must be in place in order to promote and support the take-up of IoT by user industries, build the critical mass of users needed to encourage the investments needed for massive adoption, and to create favorable framework conditions for the development of the IoT ecosystem.

Such strategy is also necessary to address any challenges that are relevant to entry into new markets and radical disruption of existing industries. Such challenges may include:

- Large investments needed to take full advantage of IoT and M2M communications.
- Creating favorable public-private partnerships and cooperation between municipalities, businesses and contractors to reduce costs and share resources.
- Avoiding industry and vendor-specific IoT platforms which could limit opportunities for SMEs and startups to participate, and increase risks of fragmentation between industries of lock-in in proprietary ecosystems, through restraints in interoperability and access to data and applications.

The GSMA's recent report on M2M in China highlights the role that governments can play in stimulating the M2M market. The Chinese government has made available special funds to accelerate the development of the IoT market. In addition, the Chinese Government plans to invest CNY3,860 billion ($603 billion) in the M2M/IoT ecosystem until 2020, according to China's R&D Center for Internet of Things (CIT-China).

Latin America has witnessed positive policy moves by regulatory bodies, such as proposed reduction of the Brazilian M2M tax, which was placing a significant burden on operators' M2M business models, and constituted a major barrier to adoption.

The Turkish government has also exempted M2M SIMs from a tax collected on any new SIM connections, which has created a positive impact on margins derived from M2M services.

We believe that maximizing the benefits of the IoT will likely require more coordination and dialogue across all sectors and stakeholders, with the TRC working closely with ministries and other sectorial regulators to create a supportive regulatory framework with the aim to stimulate the deployment and adoption of IoT and M2M applications.

Connectivity remain the key enabler of IoT and M2M ecosystem, therefore, special attention should be given to supporting communications infrastructure development to allow for the robust and ubiquitous connectivity requirements of IoT and M2M communications.

To this end, Orange Mobile encourages to adopt a pro-investment and flexible regulatory approach to be established and maintained across the IoT/M2M value chain in order to enable technical and commercial flexibility. Moreover, beyond the necessary technical regulatory framework regarding the conditions of use of frequencies in free bands or use of numbering and addressing, Orange Mobile strongly believes that regulation of the IoT market should only take place in the event of evidence of market failure.

B. Specific comments:

Without prejudice to our comments above, Orange Mobile would like to provide detailed answers to the questions below:

Q1: Is the definition of IoT mentioned previously complying with your vision and the services you provide . If not, please elaborate.

In the existing literature, a number of definitions for M2M and IoT exists and currently, there is no industry agreement on these definitions. Due to the complexity of the IoT/M2M market and the large number of players involved, the discussion on terms and definitions is still ongoing and it might be challenging to reach a uniform conclusion. However, for now, Orange Group is working with the following terms, as also supported by members of the GSMA:

- **Internet of Things (IoT):** Coordination of multiple vendor machines, devices and appliances connected to the Internet through multiple networks. Devices include everyday 'objects' such as smartphones, tablets and consumer electronics, as well as machines, vehicles, monitors and sensors equipped to support M2M services.
- **IoT Connected Services:** are those delivered via devices where the connectivity is provided by authenticating a SIM and where the service has at least one of the following characteristics:
  - Open internet or open voice communications are not the primary purpose of the service; mobile connectivity is utilised to deliver value-added functionality, or
  - Services that have a closed user group and service provider managed connectivity which excludes open internet or open voice access.
- **Machine to Machine (M2M):** Devices and appliances connected wirelessly or via IP. In most cases, communication takes place autonomously, with limited human intervention. M2M is an integral part of the IoT.

- **Machine to Machine User:** Purchaser of an M2M service who incorporates the M2M service as one component in his own products and/or services (e.g. a car manufacturer, an electricity provider who also includes a smart meter in his services).

Q2.1 Do you offer any IoT services in the Jordanian market? If Yes, answer the following:

2.1.1. Kindly, list and briefly explain those services.

Orange Mobile offers a good range of connected objects to our residential customers, including home automation, surveillance, smart wearables and virtual reality gears. Orange Mobile also offers on a standard basis dedicated M2M connectivity rates (data and SMS pools), as well as a Vehicle Tracking System service.

In addition, on a tailor-made basis, Orange Mobile can offer complex solutions such as asset tracking, data collection (eg. Census), smart metering and other Smart City services.

Q3.1: What are your expectations to the IoT traffic capacity in Jordan for the next 5 years?

We do not have any calculation available to our expectations of IoT traffic capacity at this stage. We strongly believe that a national IoT strategy or plan – as referred to in our general comments above- must be in place in order to promote and support the take-up of IoT, and consequently determine the expected level of demand for such services.

Q3.2: In which fields of implementation it's expected to have the highest "data interaction" traffic and which is expected to be the lowest?

We do not have a prediction available at this stage to indicate the highest "data interaction". Also, the field of IoT-based services is expected to be very dynamic, and it may therefore serve little purpose to attempt to determine the specific needs of any IoT-based service. To name a couple of example, however, it is expected that with future Connected Cars supported in 4G and 5G networks, aspects such as continuous connectivity, coverage, latency and reliability are factors that need to be resolved and in place in order to support such a service. We consider, from our knowledge at this time, that the field of implementation of video streaming such as video surveillance for cities, buildings, houses, etc... will need high data interaction traffic either on the pure data traffic flow or for the treatment on the video. At the opposite end of the spectra, the example of e.g. a M2M-based solution for fault detection, an action on the side of the M2M-based

solution may only be activated in case of a fault detection, and another example is that of smart meters, where an information exchange may only take place once a month or even annually.

Q3.3: 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.

a) Aspects which are fundamental to secure in order to have an IoT-marketplace (in order of importance):

1. Spectrum and bandwidth flexibility,
2. Mobility/coverage,
3. Interoperability and standardization

b) Aspects related to ensure that services, such as Connected Cars, are supported in a way that stakeholders such as users, public authorities and industry feel confident to make use of such services (in order of importance):

1. Reliability
2. Latency

c) Aspects that providers of connectivity need to ensure in order to support IoT, and for authorities to ensure adequate numbering resources:

1. Traffic capacity
2. Massive number of devices

This particular point highlights the need for the TRC to ensure that adequate numbering resources are available to mobile network operators.

d) Aspects related to end user demand

Below parameters are all important, and if none of them does not reflect the anticipations of the customers (e.g. pricing is set too high that services are not affordable, or the data rate are not sufficiently high, and the quality of the IoT-based service suffers to the extent that is does not provide sufficient value to the customers), there will be no demand.

1. Achievable end user data rate,
2. The economic factor,

3. Network and device energy efficiency, which relates to the energy consumption in both wireless devices and network infrastructure. Critical factors that affect the energy efficiency are : Solution System design, energy storage development and renewable energy technology development.

In this context, it should also be noted that when the customer buys the services, the connectivity is an inherent part of the full customer experience, but – importantly – the customer does not buy the IoT-based service due to the connectivity, but on the basis of the perceived value of the complete service, e.g. a wearable device delivers data on steps, heart rate etc. on a consistent basis.

Q3.4: Are the data rates offered in Jordan sufficient to handle the IoT traffic especially for time - sensitive services?

We haven't met any limitation to IoT/M2M traffic related to data rates after the recent Orange Mobile network improvements. Orange Mobile is continuously investing in its network to ensure the best quality of service serving market needs as they evolve.

Q3.5: Please suggest at least three categories that classify the services that reflects reliability levels that can be needed.

- Latency of the service.
- Availability and coverage.
- Speed of the connection.

Q3.6: Please classify the services in term of latency acceptance ranges.

The latency is important when the service requires a great reactivity:

1. Automotive (case of autonomous car, where safety is at stake ...).
2. Safety services; health wearables where the reception of the alerts must not be delayed.
3. Supervision services.
4. Some Smart cities or smart industries (e.g. metering).
5. Others where the delay of reception and reactivity is not critical.

For example, cars will require the shortest level of latency (and faster speed), whilst a wearable such as a pedometer would be able to accept, support or cope with a higher latency and faster speed.

Q3.7: Please list any further challenges that might affect the implementation.

We agree with the list of challenges as listed in our answer to Q3.3.

Q4.1: Do you think that at the current stage of time there should be a specific regulation for IoT and M2M?

We encourage that a pro-investment environment is established and maintained across the IoT value chain. In order to reach a global scale across consistent and reliable platforms, service providers, and IoT device manufacturers need a flexible regulatory approach that in turn would enable technical and commercial flexibility.

Orange Mobile believes that it is crucial to note that the IoT sector is a nascent industry and its value chains, business models, markets and services, are fundamentally different from traditional mobile voice and data messaging. In most cases, IoT services have a closed user group, whereby open internet or any-to-any voice communications are not the primary purpose of the service. In addition, customers are generally not a consumer, but a business that requires global distribution coverage and managed platforms for economic viability and the provision of consistent global services. Finally, these services are characterized by significantly lower average revenue per connection than traditional voice and messaging.

Therefore, beyond the necessary technical regulatory framework regarding the conditions of use of frequencies in free bands, regulation of the IoT market should only take place in the event of evidence of market failure.

Especially, regulation which prohibits particular technical or commercial approaches should not be introduced.

Q4.1.2: 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?**

- **Spectrum:** We encourage the development of a spectrum policy centering on certainty, predictability, and consistency for this nascent industry. We agree

that M2M services have different spectrum requirements. Indeed, M2M has very different characteristics, a plethora of existing and planned technologies as well as diverse spectrum usage and access methods. Mobile cellular solutions already play a significant role given that M2M can operate in spectrum allocations intended for mobile. In addition, a number of harmonised standards have been developed recently (e.g. 3GPP or GERAN) to optimise the use of mobile spectrum bands for IoT. Thus, the mobile industry is an important enabler and well placed to lead the sector, in particular for Connected Cars and Mobile Health.

In particular, machine-type communication (MTC) extensions to LTE are emerging, including category 0 devices in releases 12 and 13, providing enhanced coverage and power options, operating in licensed spectrum, which will meet a much wider range of M2M requirements. This will provide operators with greater predictability than the uncertainties implicit in license-exempt bands.

Cellular based solutions should be developed to operate in existing licensed spectrum bands, to allow operators maximum flexibility in the use of their spectrum, while providing adequate quality of service for critical applications. M2M connectivity uses wide area, local area, and personal area wireless technologies, either individually or in various combinations to meet the requirements of a given M2M application. In the near term, proprietary Low Power Wide Area (LPWA) systems, operating in a combination of license-exempt (LE) and licensed spectrum, will continue to serve some wide area M2M requirements, which are not met by existing cellular technologies. Such LE spectrum is however intrinsically not ideally suited to wide-area M2M applications: permitted power levels and duty cycles are generally low and interference risks over long distance paths are high, especially as multiple systems from different operators proliferate. As such, the inherent nature of the LE spectrum makes it so that quality of service cannot be guaranteed.

It is necessary to distinguish between M2M/IoT services, which require the use of cellular networks, due to coverage, quality of service or traffic volumes, and other M2M/IoT services which can be satisfied with the LE spectrum. Cellular networks have a central place in the development and dynamics of this market, given the growth of M2M SIM cards. Therefore, the licensing regime and the exclusive spectrum usage rights of mobile operators for these licensed frequencies (for which mobile operators paid very high prices) need to be maintained with all required guarantees and necessary protections.

Frequencies that are not subject to prior authorization or to the licensing regime (LE spectrum) are in principle used by an indefinite number of actors. Consequently, the use of these LE bands by short-range and / or low power (SRD, LPWAN) devices should be permitted under the following conditions:

i. Such devices shall not cause harmful interference to other station.
ii. They shall not be entitled to protection against harmful interference caused by such stations

If the growth in volume of connected objects is confirmed in the near future, with a forecast of billions of objects connected globally in 2020, Orange Mobile wishes to recall that it is essential that solutions based on infrastructures using frequencies in free bands do not cause disturbances to mobile or cellular networks. The protection of these networks is indeed essential to enable the development of the "IoT" market. Therefore, Orange Mobile wishes to point out that if the licensed bands were to be subject to possible experiments, it would be essential to ensure that these types of experiments are well defined and limited in time and that mobile operating systems using the adjacent bands are well protected.

- **Privacy:** Orange Mobile believes that consumer confidence and trust can only be fully achieved when users feel their privacy is appropriately respected and protected. As stated by GSMA to the BEREC IOT consultation, " There are already well-established data protection and privacy laws around the world, which have applied to mobile operators for years".

  IoT services typically involve more parties than simply mobile operators, such as device manufacturers, online platforms and even the public sector. It is important that there is regulatory clarity and legal certainty around IoT services and that privacy and data protection regulations apply consistently across all IoT providers in a service and technology-neutral way."

  Due to the involvement of different parties in the IoT value chain, we believe that the Personal Data Protection Law, which is currently under review by the government, shall constitute the required legal framework to protect privacy and achieve trust and confidence in IoT services.

- **Numbering:** We believe that numbering resources for IoT connected services are not scarce. The GSMA further noted that at present there is already widespread industry support for roaming M2M devices that use 15-digit MSISDNs. Standardized support in the core network and roaming support systems, together with a competitive roaming marketplace, have ensured that

service providers will not encounter any significant technical barriers in deploying IoT connected devices using 15-digit MSISDNs. Moreover, the use of global ITU numbering resources is also an important alternative as a number of operators have deployed services based on these resources. As such, flexibility is essential as different services or M2M users may have different requirements. Both, extra territorial use of numbering resources and international global numbers are being used to deploy IoT connected services. The TRC should refrain from introducing any undue restriction or administrative barriers related to the assignment and use of numbering resources, as it would act a barrier to the roll-out of a M2M market.

- **Business models and competition:** Orange Mobile believes that all parties should have the flexibility to select a model that best facilitates a rapid and economically viable deployment of IoT services and provide a platform through which IoT customers can deploy high quality services worldwide while maximising economies of scale.

  No specific model should be preferred, mandated, or imposed by any type of regulatory action. All deployment model alternatives for IoT connected services considered by mobile network operators have their merit. The ultimate choice of deployment model depends on a number of factors, such as needs of the mobile network operator, the IoT service provider and the end-user, the scale and geographical footprint of the deployment, the type of IoT application, the device lifetime, its accessibility, and the bandwidth requirements.

  Yet, Orange Mobile believes that it is essential for competition that the TRC recalls the obligations to which IoT service providers are subject to when their activity can be described as an operator activity. We believe it is essential to define the responsibilities of each set of players.

  In additions, permanent roaming should be considered as one of the viable connectivity models which facilitates the creation of the IoT market across border.

Q4.2: How can you solve the above mentioned challenges that face the consumers?

Please refer to our General Comments.

Q4.3: What indicators and when do you think is the right time to regulate IoT?

Please refer to our answer to Q4.1 above.

Q4.4: 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?

Please refer to the answer to question Q4.1.2.

Q4.5: When the review should take place to specify the need of taking an action?

Please refer to the answer to question Q4.1.2.

Q4.6: 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)?

The growth of the IOT will be based on a variety of technologies including wireless technologies. Wireless connectivity technologies are numerous and varied, and the use of one or the other is often primarily determined by the scope of the network envisaged. Some use cases also require the combination of wireless and wired technologies to connect equipment to private or wide area networks.

Among the wireless technologies deployed over long distances, type MAN or WAN, Orange Mobile primarily considers:

- Conventional cellular networks (3GPP14): 2G, 3G, 4G,
- Low Power Wide Area Network (LPWAN): LoRA,
- LPWAN solutions via cellular networks (3GPP): LTE-M, NB-IoT, EC-GSM-IoT.

Q4.7: Do you think that the spectrum and backhaul capacity you have will meet the demand of the IoT needs?

Orange Mobile is continuously investing in its network to ensure the best quality of service serving market needs as they evolve.

It is worth mentioning that the prices asked for the Spectrum can limit the extension of our capacities to deliver fast mobile broadband. Orange Mobile

urges TRC of the necessity to review the spectrum acquisition fees, and also to issue regulatory framework of spectrum access sharing.

Q4.8: Regarding the millimeter wave bands, do you think they will be useful and meet the requirements of IoT?

Please refer to the answer to question Q4.1.2.

Q4.9: When do you think such development of mobile networks as mentioned previously (in section ii switching and roaming) will be needed in Jordan?

We do not have expectations of M2M related developments at this stage. We strongly believe that a national IoT strategy or plan must be in place in order to promote and support the take-up of IoT, and consequently determine the expected level of demand for such services.

Please refer to our general comments above.

Q4.10: Is there any need for a regulatory framework by the TRC to regulate the IoT roaming issues?

Q4.11: Do you think that the current signed roaming agreements are appropriate to encourage IoT services in Jordan? Or do those agreements need update?

Answer to Q4.10 and Q4.11:

Roaming for IoT should not be subject to the TRC Roaming Regulation and should be negotiated on a commercial basis. We believe that the evolution of IOT connected services delivered through mobile communications networks should be progressed through the current process of bi-laterally agreed commercial negotiations. There is no need for TRC intervention without prior demonstrable evidence that the industry is failing to address market needs, for example by refusing to negotiate roaming agreements. Unit Cost per object is an essential parameter in the competition between connectivity providers for IoT and this is why price levels must be set by the market. This is all the more important as the market for IoT services is still in its infancy. All actors should have the flexibility to choose the models best suited to their needs. No specific model of supply should be imposed, promoted or prohibited by regulation.

Q4.12: Is your company welling to dedicate SIMs for M2M Communications? if Yes, will the cost rates vary from normal roaming services?

Orange Mobile will also consider the "Embedded SIM" for some specifics services. Solutions for remote updating (over-the-air) of SIM cards should facilitate the development of the Internet of the objects with the ability to load a new operator subscription on SIM cards integrated in equipment. The generalization of this type of solution in the IOT world has been facilitated by the creation of standards enabling interoperability between products and a global adoption in the market of this type of solution.

Orange Group and other global operators have worked closely with the GSMA to develop the specifications for the remote delivery of the "Embedded SIM". This solution resolves the issue of switching connectivity providers for connected IoT terminals.

The "Embedded SIM" provides the technical solution to eliminate the need to physically change the SIM. Remote provisioning allows service providers to choose a connectivity operator later in the product lifecycle, for example, when deployed at the customer's location or at the time the deployment country is known. It also facilitates the change of connectivity operator. The GSMA specifications for the Embedded SIM are suitable for multinational mass deployments in cases where the connectivity operator cannot be selected at the outset when the deployed terminals have a long life or when the physical change of SIM is impractical.

Q4.13: Is there any need to draw a distinction between person-to-person communications and IoT connected devices in terms of roaming?

Due to the evolution and the specificity of the IoT in terms of traffic it is necessary to distinguish between person-to-person communications and IoT connected devices for roaming purposes.

Orange Mobile considers that IoT roaming should not be regulated and should be negotiated on a commercial basis.

Q4.14: 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.

In terms of ensuring that a customer is able to change provider, it is the view of Orange Group that the specifications of GSMA for the remote provisioning of

Embedded SIMs is an efficient technical solution to enable a smooth change of provider and avoid lock-in mechanisms.

Q4.15: When do you think that regulating market competition issue of IoT in Jordan will be a critical issue?

See responses to Q4.1 and Q4.1.2.

Q4.16: 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.

See responses to Q4.1 and Q4.1.2.

Q4.17: 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.

The market for IoT/M2M is indeed global and not national, as such it should be left to market actors, such as e.g. manufacturers of IoT-based products and services as well as connectivity providers to drive up competition through natural market forces instead of formal regulation. This will provide better services and prices to citizens and create innovation in the market place.

Q4.18: Do you have a policy for visibility and secure management of "Things" on your network today?

Q4.19: Are you collecting management or visibility information from the "Things" on your network?

Q4.20: How are you collecting security and operations data about "Things" on your network?

Q4.21: How would you rate your ability to provide security to the "IoT" services?

Answer to Q4.18 to Q4.21:

At this point in time operational data available regarding "things" connected to Orange Mobile network through M2M connectivity is similar to data available for devices connected through standard mobile data services. However, Dedicated APNs available for M2M users provide an additional level of security. Dedicated

APNs can provide a private communication for specific IoT community that assures closed access to this APN from the IoT end points only.

Service platforms (eg. Vehicle Tracking System) usually provide additional visibility and management features specific to the concerned services.

Depending on market needs and volumes, Orange Mobile might in the future deploy dedicated IoT/M2M connectivity and data management platforms providing enhanced flexibility, visibility and data handling capabilities.

Q4.22: What controls do you plan on deploying in the next 5 years to protect against security risks?

Q4.23: What do you think the greatest security threat to the IoT will be over the next 5 years?

Q4.24: 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?

Q4.25: Do you think that there is a need for security protection regulation to be issued in the current time?

The following is the answer for question 4.22, 4.23, 4.24 and 4.25:

Orange Mobile believes that in order to increase IoT security, a solution that both facilitates industry innovation and the adoption of security-by-design is necessary. In this regard, regulation should be used with caution in order not to hamper innovation, and it should be mentioned that the French regulator ARCEP concluded – in relation to a consultation on IoT - that it was too early to specifically regulate the IoT sector, as it is currently very innovative and experimental. However, regulation may be used to facilitate the adoption of security standards by industry.

Orange Mobile believes that security and trust are essential conditions for the development of the IoT market, and the commercial strategy of Orange Mobile relies on a trust relationship with its B2C clients that includes transparency about data usage and data protection as well as a rich cybersecurity offer for the B2B market. Orange Group has a comprehensive IoT offer (object catalog, IoT networks, data management infrastructure) of which the components have been audited and are securely hosted and monitored, etc.

Orange Group has a broad catalogue and know-how in security processes and solutions that can be used for any project, and the "Orange CyberDefense" can

help companies build security for their IoT services through audits and consulting.

Furthermore, Orange Group continues to conduct research in security and in particular IoT security with the aim of designing the next secure operating systems for objects, and lightweight cryptography adapted to small objects. Orange Group allocates considerable resources to our participation and contributions in various security-focused Working Groups in standardization bodies such as 3GPP, ETSI and the LoRa Alliance and within the GSMA, Orange Group has contributed to the definition of security recommendations for the IoT and of a self-assessment questionnaire. Additionally, Orange Group is also an active member of the AIOTI (Alliance of IoT Innovation), initially established by the European Commission to facilitate an exchange between the EC and industry, and now an independent European business association on aspects related to the IoT, including that of privacy and security.

Q4.26: 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?

Please refer to answers to Q4.27 below.

Q4.27: Are you dedicating Gateways, IPS, and Network monitoring systems to your connected "Things"? Or you are utilizing your current Network infrastructure and systems?

At this point in time Orange Mobile is connecting "things" to its network through M2M connectivity using the current mobile Network infrastructure and systems. However Dedicated APNs available for M2M users provide an additional level of security.

Service platforms (e.g. Vehicle Tracking System) provide additional network management features specific to the concerned services.

Q4.28: What kind of encryption algorithms your organization uses for your network communications?

Orange Mobile is deploying the needed ciphering algorithms in all radio access types 2G/3G/4G to assure encrypting the radio path of IoT traffic flowing in the 2G,3G and 4G radio paths. To give an example, in 2G data network Orange Mobile is using encryption algorithm GEA/3, in 3G data network Orange Mobile is using UEA/1 and UEA/2 as encryption algorithms, in 4G radio we are using EEA/1 and EEA/2. This encryption covers user signaling and payload traffic over

the radio path. The IoT devices qualified by device entry regulation should be able to support the most recent encryption algorithms.

Encryption over the internet is subject to the device capabilities, type and criticality of IoT application and such a traffic is end user device and application defined and thus neutral to the mobile network since encryption/decryption is realized at end user device and application sides.

Q4.29: 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?

Yes. Orange Mobile data privacy policies are compliant with international best practices.

Q4.30: How would you rate your ability to protect privacy of the "IoT" data?

Orange Mobile data privacy policies are compliant with international best practices.

Q4.31: What controls do you plan on deploying in the next 5 years to protect data privacy?

We do not have any expectation yet. This shall depend on the existence of national agenda which shall trigger greater demand for IoT services.

Q4.32: Do you think that there is a need for data privacy protection regulation specific for IoT services to be issued?

No, the Personal Data Protection which in the process of being finalized by the government law will be sufficient once released.

Q4.33: 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.

To strengthen the trust of citizens, consumers, businesses and other persons and organizations on the demand side in their networked day-to-day and commercial life, basic requirements for security and privacy are called for that minimize risk, are neutral in technological terms, and remain open to innovation.

These requirements need to embrace all sectors and all the components, ranging from simple devices such as smart thermostats to complex IoT systems such as connected cars. They also need to address the overall system architecture in order to enable devices to communicate in a manner that ensures data security

and privacy to common standards. The resulting rules shall guide common tools, approaches and instruments such as standards, certification, self-regulation, and labeling.

It is imperative that such levels of assurance are developed at international level, as the predominant number of IoT-based services will global by nature.

Q4.34: 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?

We use currently allocated numbering range for IoT/M2M.

Q4.35: 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.

At this point in time we do not see a need and rationale to specify a dedicated numbering range for IoT. Current M2M deployments are based on utilizing the existing numbering resources, which are currently considered sufficient.

However, given the cost of implementing an additional range or length, Orange Mobile believes that in the short to medium term, the usage of the existing mobile number ranges can be preferred. However, if the growth of M2M is larger than expected or if the capacity would not be sufficient, a new numbering range would indeed be needed, taking into consideration that there is still a space on the current mobile ranges by adding three digits for SN in mobile services, or alternatively reserved mobile ranges for future use could be utilized (i.e. 071xxxxxxx – 073xxxxxxx).

In principle, Orange Mobile support addressing the issue of designating special numbering range for IoT/M2M services given future potential demand for such services. However, given the current low demand for such services, we recommend the following approach:

1. Allocation of numbering capacities for M2M services should only be limited to licensed operators.
2. Continue the current usage of mobile and geographic numbering capacities for M2M services up to the point where high demand for such services that require the usage of the dedicated numbering, or adequate capacity is not sufficient or may cause depletion to the current numbering resources.
3. TRC should ensure that the M2M number range(s) are not used as an alternative to existing number ranges to escape regulatory requirements.

4. Any new IoT/M2M numbering ranges(s) should not specify digits for type of service or operator as it will be very limiting due to the fact that the IoT/M2M communication is IP based communication and the associated E.164 number is recognized for own operator charging/customer services management.
5. Any new range of numbers should be applied to existing and new IoT/M2M customers, since such change in numbering are not user impacting (E.164 is not SIM / user peripheral defined) but only recognized within internal operator customer relation management systems, and in order to maintain a consistent National numbering Plan.

We would like to emphasize that Mobile network codes (MNC) numbering allocation policies should not be changed, i.e. MNC sharing and allocation for non-mobile operators should not allowed. Despite that the new ITU recommendation E.212 gives more latitude to National Regulatory Authorities, it does not mandate more flexible criteria, and the rationale for having more flexible criteria on such scarce resources globally remains weak, changes to MNC allocation rules should only be contemplated if all other means have been exhausted to meet the requirements of the market. Moreover, sharing and allocation of MNCs for fixed operators will cause distortion to the mobile and fixed sectors, and will encourage one sector at the expense of the other due to significant differences between the types and values of returns and fees applied in both sectors. In addition, we would like to point out that technology and standards did not yet define clear services in fixed network or fixed/mobile convergence that would need the use of MNC as part of user identification to allow for service authorization and access.

Q4.36: Do you think that the late migration to IPv6 will limit the IoT expansion?

Yes.

Q4.37: Do you agree to use a specific code (MCC) in IMSIs permanently for M2M services abroad?

As assessed by GSMA, its specification for remote provisioning of Embedded SIMs is more efficient and is likely to have lower implementation costs.

The GSMA specification for remote provisioning of Embedded SIM addresses concerns regarding the ability to switch connectivity providers for IoT connected devices. Technical solutions for changing connectivity provider are available today that eliminate the need to physically replace the SIM or to loosen MNC allocation policies. The use of a remote provisioning capability provides a

solution that enables providers to select a connectivity partner at a later stage in the product lifecycle, i.e. when it reaches its customers, potentially in another country. The GSMA Embedded SIM specifications were developed specifically for large multi-national deployments where it can be challenging to provision connectivity from the outset, or when deployed devices have a long lifetime and/or are deployed in locations where physical SIM replacement is not practical.

It has to be noted that the basis for growth in M2M-devices is at very small cost per unit for the manufacturers of IoT-devices. So in order to make M2M and IoT-services cost-effective, the Embedded SIMs will make the costs for the device manufacturer and the mobile network operator at the lowest possible level.

On the other hand, it should also be noted that some devices will be equipped with SIM-cards at the place of manufacturing, which could be any place in the world, and may not be based on Embedded SIM specifications.

M2M devices might use global E.164 and E.212 numbering resources assigned directly by the ITU (i.e. Country Code 882/883 for E.164 numbers and MNCs under MCC 901 for E.212 numbers). These ranges are not belonging to any country and it can be requested directly from the ITU but this might impose additional burdens on IoT service providers (e.g. they should be a member of ITU).

For example, a fridge manufacturer in Asia may have a contract for a number of SIM-cards which contains IMSIs. The SIM-card is installed in the fridge (potentially by a third party) to provide the consumer with information in case of deviations of the temperature inside the fridge. The fridge is shipped to x-number of countries globally. From the point in time that the IMSIs are issued to the manufacturer, it is impossible for an operator to know beforehand where these IMSIs will be used at the end of the chain and maintain this information over time (change of country, etc.) Further, it may be extremely challenging for the operator to actively monitor the level of traffic derived from these SIM-cards. The low revenue per unit may indeed not facilitate that this is economically feasible.

Therefore, and in order to consider the permanent roaming as one of the viable connectivity models, we strongly believe that devices equipped with SIMs that are not based on GSMA's Embedded SIMs should be allowed to enter the Jordanian market for M2M communications purposes subject to notification requirements so as to have more visibility over extraterritorial E.164 and E.212 numbers used in Jordan.

Q4.38: 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?

Orange Mobile considers that MVNO arrangements should not be regulated and should be negotiated on a commercial basis. IOT services will be part of the commercial negotiation between the mobile network operator and the MVNOs based on a global business case analysis.

Q4.39: 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?

IPV6 is not currently being used.

Q4.40: 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?

At the moment Orange Mobile uses the IMSI and IP address (private or public) of the devices using IoT and M2M services communication. MAC addresses are not used. The MSISDN is used only for billing and customer relation management services.

Q4.41: Any recommendation about the Addressing and Numbering for IoT services provided by non-telecommunication licensed companies?

Due to the scarcity of numbering resources and MNC-codes, Orange Mobile will recommend that these resources stay regulated by the TRC. Also please refer to our answer to Q4.35 above.

Given the radical changes to mobile network architectures which are under way with the advent of so called "all-IP networks" and VoLTE/5G with potentially new opportunities for identities other than numbers such as IP addresses or alphanumeric identities ("email-like" formats), it would not be necessary or desirable to rush into a change of numbering formats. TRC should therefore keep a close look at the development of IPv6 for the longer term where IPv6 addressing will become important and the target instead of E.164 numbering for M2M communications.

Orange Mobile believes that a long term solution for M2M shall be IPv6 where numbers/addresses other than E.164 numbers would be used for IoT/M2M applications. With the proliferation of IPv6, there will be no limit of addressing resources.