Representing:

Self

Organisation (if applicable):

What additional details do you want to keep confidential?:

No

If you want part of your response kept confidential, which parts?:

Ofcom may publish a response summary:

Yes

I confirm that I have read the declaration:

Yes

1. IoT definition, applications and demand:

The ongoing transition from M2M to IoT can be compared to the transition from proprietary communication networks to the Internet in the 80's.
Today's M2M applications tend to have a centralized, client-server architecture, i.e. one-to-many, therefore the number of interconnections to manage remains proportional to the number of connected objects.
A drastic change arising from the IoT transition will be the advent of "many-to-many" distributed architectures wher the number of interconnections to manage will raise exponentially compared to the number of involved objects.
Furtthermore, this will require a more dynamic management of authorizations to enable applications to access data from connected objects.
This will also generate an evolution of M2M security threats and solutions to address comparable security issues as encountered today on the Internet:: Frequent software patches to address new discoverabilities, sophisticated protection levels, etc, with additional challenges deriving from IoT constraints in terms of energy drain, computing power, bandwidth considerations etc.

2. Spectrum requirements :

The hige variuty of M2M appliactions has to be accomodated, which may require a choice of communications technology fitting different demands in terms of bandwidth, latency, overhead, packet size, energy efficiency in particular.
From this perspective, location specific approaches to spectrum allocation may be preferable.
Accomodation of coexistence should deopend from the characteristics of the specific communication technology considered.

3. Network-related issues:

4. Security and resilience:

Security requirements of M2M applications vary widely, and should be guided by threat analysios specific to each deployments. A challenge today is that M2M/IoT applications are generally conceived by industry experts who have limited or no IT security awareness.
As noted above (see 1) IoT security is even more demanding than Internet security because of sevices limitations and potential sensitivity of applications such as critical infrastructures.
Such sensitive applications will require certified levels of security for protecting the secrets on which security relies, and depending on device exposure to potential attackers (no exposure, remote exposure, or physical control) should rely on more developerd hardware mechanisms than what is implemented in today's general purpose computers.
The management of authorizations for applications to access data from connected objects will require evolved solutions that can cope with the rising number of interconnections and their dynamicity.

5. Data privacy:

The issue for data privacy is that connected objects will expose data about our lives without our awareness.
Addressing this issue will require that sappropriate controls be given to exposed individuals, throughcapabilities for users of connected objects to configure them according to their desires.
A basic principle for privacy prorection that will need to be enforced in IoT is data minimization, i.e. sensitive data should not be exposed any further than absolutely required. This can be achieved only by local processing to extract the desired information and local storage.

6. Numbering and addressing:

7. Devices:

Device requirements vary widely between applications.
In terms of security, one guiding parameters is their exposition to potential attacklers. Some devices are under physical control of potential attackers while onthers are only remotely accessible at best. In any case proper protection of the secrets that are the seed for security must be ensured.

8. Digital literacy:

9. Data analysis and exploitation:

Contrary to the dominant trend towards centralized cloud storage and processing, resolving the IoT challenges will require highly distributed approach to data acquisition, analysis and storage, This is especially necessary to preserve privacy.

10. International developments:

Standards such as oneM2M are starting to emerge, that will provide the required interoperability framework to enable the IoT to become reality. Significant efforts stiull need to be made to break the clustered approach traditional to industrial standardization (IEC vs.

ISO vs. ITU depending on sector) and develop interoperable semantics and ontologies among different domains.

11. Ofcom’s role :

12. Additional comments: