	Response by JRC Ltd to Ofcom's Call for Information Promoting investment and innovation in the Internet of Things	**JRC Ltd** **Dean Bradley House** **52 Horseferry Road** **London SW1P 2AF** ☎ 020 7706 5199 020 7222 4862 info@JRC.co.uk

Call for Input

IoT definition, applications and demand:

Definition of the M2M and IoT:

The Joint Radio Company (JRC) would like to highlight that the utilities have been operating resilient-machine-to-machine (RM2M) systems for approximately 50 years. These systems include the supervisory control of, and data acquisition from, remote infrastructure. NB: these remote infrastructure sites are often far beyond the service coverage areas that may be considered economically viable by non-private mobile radio (PMR) operators.

The Joint Radio Company (JRC) therefore suggests that, like RM2M, the broader terms of machine-to-machine (M2M) and the Internet of Things (IoT) can both be described as:

'Any existing or future fibre, wired, wireless, or combination of technologies that enable connected devices to exchange information and perform actions without the manual assistance of humans'.

Spectrum requirements:

Smart Meter spectrum:

The Joint Radio Company (JRC) would like to highlight that there are two planned UK smart meter systems. Arqiva will provide the network for Scotland and the north of England using long-range radio communications operating on a number of its existing licensed 12.5 kHz channels within the 412 to 424 MHz spectrum. Telefónica's network will cover the rest of England and Wales using existing O2 mobile cellular radio communications spectrum plus Connode's mesh radio technology, within existing short-range licence exempt 868 MHz spectrum, to supplement connectivity to the hard to reach locations.

The long-term spectrum requirements for smart metering for England, Scotland, and Wales have already been considered by the two suppliers; with the current spectrum access arrangements being considered sufficient.

Smart Grid spectrum:

Although some consider that public / mobile communications networks could meet the future communications requirements of the utilities, the Joint Radio Company (JRC) notes that the number, scope, and sophistication of cyber attacks on the information and communication systems of the utilities globally is increasing. Whilst the existing self-managed spectrum and necessary security measures are continually being enhanced to defend against such attacks, it emphasises that future utilities systems[1], including smart grids, will continue to need resilient data networks which currently requires access to licensed dedicated spectrum.

The benefits of utilities' continued access to licensed and self-managed spectrum for these highly specialised radio systems is that they can be designed, installed, and maintained to:

- cover unpopulated geographical areas of the UK which have vital utility infrastructure;
- have instant and guaranteed access;
- remain resilient to Best Practice levels, enabling them to continue to operate correctly during and after natural and / or man-made disturbances, e.g.:
  - by using communications link diversity;
  - by using end-to-end separation;
  - by having 72-hours mains-power independence along their entire communications chains;
- ensure they, and the transmitted data, have high levels of security and integrity;
- stringent end-to-end latency requirements:
  - 10mS end-to-end latency is required for the sensors and actuators used in the power industry's high voltage protection circuits;
- ensure low jitter and synchronous requirements;
- low to medium data rates, e.g. 9.6 kb/s;
- have longevity of life and support, e.g. 10 to 20 years; and
- are hardened to ensure reliable operation in severe environmental conditions (including electromagnetic disturbances).

With the security and resilience of utilities' communications being vital to the continuous availability of services critical to society, JRC represents utility interests in the expansion of current self-managed spectrum within the 450 to 470 MHz band, to 2 x 3 MHz to be confident of meeting the utilities' future intelligent networks spectrum requirements. (Ideally, this 2 x 3 MHz of spectrum will be harmonised with European arrangements.)

This 2 x 3 MHz is a small amount of spectrum when compared with that to which the mobile network operators (MNOs) have access, especially when compared with the additional ~100 MHz of spectrum that is being considered for additional public mobile spectrum. This small increase in 450 to 470 MHz utilities' spectrum is possible because unlike the consumer and commercial markets, utility systems do not require broadband data rates and typically only transmit low bit rates. This enables the utilities to use licensed 12.5 kHz (0.0125 MHz) channels rather than the MHz-wide channels used by mobile broadband systems.

1 http://eutc.org/system/files/UTC_private_file/EUTC%20Spectrum%20Position%20Paper-9April2013.pdf

Security and resilience:

The European Union Agency for Network and Information Security (ENISA) in Article 13a of its Technical Guideline on Security Measures provides additional insights:

Definitions used for the utilities and other communications systems:

Paragraphs 1 and 2 of Article 13a state:

“1. Member States shall ensure that undertakings providing **public communications networks or publicly available electronic communications services** take appropriate technical and organisational measures to appropriately manage the risks posed to **security** of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

2. Member States shall ensure that undertakings providing **public communications networks** take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks. […]”

Additionally, the European Union Agency for Network and Information Security (ENISA) highlights within its Technical Guideline on Security Measures (Technical guidance on the security measures in Article 13a - Version 2.0, April 2014) that '**One size does not fit all**'. Adding, 'The reason is that the electronic communications sector is very diverse; large incumbents, small service providers, black fibre operators, virtual mobile network operators, ISPs offering only DSL, et cetera. **In each setting the risks are different and it is up to the providers to assess the risks and decide which are appropriate security measures to take**'.

Considering the above, appropriate care should therefore be taken when considering the definitions for security and resilience shown within the consultation document, responses, and subsequent document(s) because they may not be appropriate definitions for all communications systems, e.g. the definitions used for non-public communications networks such as the more stringent 'Best Practice' requirements of the utilities networks.

CPNI's definitions for Best Practice and Good Practice:

The Centre for the Protection of National Infrastructure (CPNI) document 'TELECOMMUNICATIONS RESILIENCE GOOD PRACTICE GUIDE' Version 4 (MARCH 2006)[2] states:

“Best Practice is defined as those measures that can be taken to guarantee resilience, irrespective of cost. Good Practice can therefore be defined as those measures which can be taken to provide a degree of resilience commensurate with the Corporate risk strategy.”

Also, “High levels of resilience incur additional costs in equipment/line plant and process overhead and not every business or institution can therefore justify the cost associated with Best Practice. Some will therefore choose a level of Good Practice commensurate with the risk.“

2 http://www.cpni.gov.uk/documents/publications/undated_pubs/1001002-guide_to_telecomms_resilience_v4.pdf

It is understood that, perhaps because of the otherwise substantial increase in cost, existing mobile network operator's (MNO) systems only work to Good Practice levels; and then only where there is good signal coverage between the base station and the mobile phone. Despite the actual distance, this connection is often referred to as the 'last mile'.

The CPNI document's definition of last mile, states:

“The ‘last mile’ (between local exchange and customer premises) is the key to the resilience of a business telecommunications network”. The provider’s network has a high level of built in resilience resulting in few failures. The last mile connection to the customer however is usually a single point of failure, often because there is simply no alternative route. It is also the most exposed part of the network to external interference or disruption. Any company with more than one route into the Provider’s network has more than doubled its survivability.”

The same single point of failure problem applies to the wireless connection between a base station and a remote station. Despite the higher cost to meet this necessary Best Practice resilience requirement, this recognised weakness requires the utilities' communications networks to typically have at least two diverse routes to its remote stations.

*The CPNI document's advice on 'Deciding what resilience is needed'**:***

“Those systems that are mission critical need to have specific resilience measures in place. A realistic risk assessment of the corporate communications systems will identify these. … This section provides information that the reader can use within a risk assessment exercise.”

This risk assessment includes 11 recommendations. Those recommendation include the following topics:

- Availability Definition;
- Services judged to be medium or low risk;
- Services judged to be mission critical and high risk;
- Single Point of Failure;
- Transparency;
- Dependency on a single Provider; and
- Due diligence in selecting the Provider.

Future utilities communications systems:

The utilities use similar methods to decide which systems may be used for their communications networks now and in the future. The important element for utilities in terms of their communication networks is that they remain under their control and direction. When using radio systems within their communications networks, access to licensed radio spectrum is vital to ensure integrity of operations. Increasing the utilities current 450 to 470 MHz access to 2 x 3 MHz will greatly assist in meeting their obligations to meet government policy aspirations.