Silver Spring Networks'
Response to Ofcom's "Promoting investment and innovation in the Internet of Things" Call for Input

Silver Spring Networks (SSN) is grateful the opportunity to respond to Ofcom's Call for Input regarding the Internet of Things (IoT). We believe that we have a relevant point of view, having deployed nearly 20 million communicating devices across what is often referred to the "Industrial Internet", a category of the IoT with a set of requirements that is distinct from the consumer IoT. We are grateful, too, to Ofcom for taking a leading role in promoting access to useful, license exempt RF spectrum across Europe (e.g., TV White Spaces; additional SRD spectrum for M2M, smart cities, smart grids, smart meters); this thought leadership coupled with real effort will deliver great societal value to consumers and citizens.

We categorize our input very generally in accord with the broad outlines of the CFI.

Defining the IoT

- We agree that wireless technologies are the future of IoT, allowing the billions of devices anticipated to be deployed to be easily connected.
- Many technologies will be involved including mains powered, to battery, to energy scavenging. Therefore, the transmission of power using RF has no place (especially at VHF/UHF) – this spectrum is too valuable to waste.
- Industry will provide infrastructure, both as private networks, and, ultimately, publically accessible networks (such as in South Korea).
- Industry will decide degree of openness on the protocols at different layers in the stack.
- There needs to be a single national approach to the roll out and regulation of the IoT, else the management of the network(s) will become too complicated.
- Security is a huge concern around the IoT. End devices will become vulnerable if not upgraded and protected. Given that devices will not be monitored and could remain compromised for months of years, the deployment and management of state of the art security techniques and protocols will be absolutely necessary.
- End users of these services will also need to understand what data is being gathered, transmitted and stored on their behalf.

Radio Spectrum Allocation and Management

- Ofcom has taken the initial steps in making 870 – 873 MHz commercially available. We encourage Ofcom to go further by allocating 873 – 875.6 MHz, also. We think that the demand and commercial success of license exempt, sub-GHz bands in the Americas, Australia/New Zealand, Southeast Asia,

China, and Japan is indicative of the demand that will be seen in the UK and across Europe.

- We also encourage Ofcom to carefully consider ensuring that operating parameters such as duty cycles are not neutered such as to render allocated spectrum as less useful. The consultation on NRPs is a step in the right direction and the considered inquiry should be applauded.
- Nevertheless, the IoT will require significant amounts of licence-exempt spectrum at UHF and VHF – and at liberal access conditions. Managing an eco-system with billions of devices, with devices and technologies produced by hundreds of companies will simply not be possible without the availability of sufficient spectrum.
- Cellular operators can continue to offer similar services using managed spectrum. But the market decide which solution is needed for which Use Case. We believe many will enjoy the simplicity of services offered by licence-exempt spectrum.
- Efficient use of (licence exempt) spectrum is being considered in SRD/MG, where they are constantly striving for regulations that encourage higher spectrum efficiency, and are latterly considering Cognitive radio techniques as part of the 6th Update to the standing mandate.

IoT Policy

- We think that security is paramount in large-scale Industrial Internet applications such as metering and streetlights. And we think that "sunlight is the best disinfectant" is not just an interesting phrase. Many delay-tolerant, extremely small payload implementations that have been procured or are deployed today in the UK have serious security deficiencies, many of which could be revisited and remediated. The intersection of IoT and critical infrastructure is an area for policy diligence. Ofcom and other relevant entities should set a lowest common denominator for Layers 1 – 3 in terms of minimum security. We would be happy to further discuss.
- Legislation might force providers of solutions to declare the level of security of their solution so that users can decide whether to trust the technology for particular uses.
- Vendors of equipment should be required to provide robust security that can be malleably changed according to policy. Silver Spring has views on security policy, but we think it more important to provide robust toolkits that can be manipulated to meet policy objectives. We think that Ofcom should be mostly concerned with the "lower layers of the stack" in the realm of mandating minimum standards for security.

Address Assignment and Management

- First, we think that the world will invariably move to IP in every endpoint, in particular IPv6. We find it puzzling when large procurements (particularly government procurements, which can help shape a market) do not insist upon this, irrespective of whether or not global routability is a requirement. The economics behind decades of IP R&D and implementation expertise, network management, and application layer diversity should not be discounted. Adaptation layers such as 6LoWPAN for constrained link layers have proven that on-air efficiencies can be delivered.
- re NAT: in practice, we think building massive greenfield IoT networks requires large namespaces and numbering headroom. Silver Spring's implementation was built upon IPv6 in 2004. With that said, we are skeptical that all but a very tiny percentage of IoT devices will be global routed and will require globally routable (i.e., public) IP layer addressing, irrespective of the use of IPv4 or IPv6. We would be interested in seeing the evidence (i.e., use cases) for global routing of things such as in-premise devices such as thermostats or light bulbs or even motor vehicles. Global routing should not be precluded as a configuration or policy option, but is there an authoritative projection for the number of IoT devices that will not be behind a gateway? Competent implementers can deliver this today, but is there a market demand?
- Global routing will be based on end-user requirements and policy of the provider. There is no need for mandates here.
- We think stateless auto-configuration in IPv6 is a good thing for ease of management.
- Policy around network layer addressability assumes a "sanctioned" network layer, in this case, IP or telephony. LTE is packet based and it might be a bit of unnecessary work and effort to conflate a request for additional telephone numbers with the IoT.
- Finally, therefore, we believe that no further action needed from Ofcom for the introduction of additional telephone numbering space.