To: The National Telecommunications and Information Administration
From: Michael Jung, Policy Director, Silver Spring Networks (mjung@ssni.com)
Date: May 23, 2016
Subject: Internet of Things

INTRODUCTION

Silver Spring Networks commends the National Telecommunications and Information Administration for demonstrating leadership by issuing Docket No. 160331306–6306–01 regarding *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*. The Internet of Things represents a powerful opportunity to harness the power of communications and information technologies to deliver new benefits and capture valuable efficiencies by connecting infrastructure in unprecedented ways. With the support of forward-thinking government policies, US companies and citizens can be well-positioned to capture first-mover advantage in this important new sector.

Silver Spring Networks (SSN) is the recognized market leader in networking major infrastructure for global utilities and cities. By many measures, SSN is arguably one of the most successful IoT company in the world today. Our hardware, software, and services have been proven in the field across over 23 million endpoints delivered around the world. SSN was founded in 2002, went public in 2013, and employs over 600 people today, with headquarters in San Jose, CA and offices in Chicago, San Antonio, Melbourne, Sao Paolo, Paris, Singapore, and London.

SUMMARY

The IoT, although based on the internet, relies on different fundamentals, including:

- **Interfaces & Importance**: People vs Things; important Things vs gadgets
- **Performance Priorities**: Network bandwidth vs latency and reliability
- **Network Architecture**: Leverage the smart grid to maximize IoT access

To support and accelerate IoT development, SSN recommends policy priority be given to:

- **Spectrum**: Ensure continued availability and consider additional expansion of unlicensed wireless spectrum, especially in the 902-928 MHz band, for IoT in the US, and support efforts to encourage harmonization of this spectrum for IoT abroad.
- **Cybersecurity**: Invest in human capacity across industry and government to ensure cybersecurity for the IoT.
- **Access**: Avoid creating an “IoT digital divide” and better utilize already-deployed assets by leveraging networked utility infrastructure to enable universal IoT access.

UNDERSTANDING THE IOT

The term “Internet of Things” (IoT) generates equal measures of excitement and confusion. The excitement is born from the IoT’s tremendous potential to transform our way of life, but the confusion should be addressed early on before misunderstood meanings lead to misguided policies. Much of the confusion arises from the incorrect notion that the word “Internet” in the “Internet” that we all use today and the “Internet of Things” that we dream about for tomorrow refer to the same thing.

Although the IoT utilizes many underlying technologies in common with the Internet, such as routing and addressing schemes, the IoT and the Internet differ in important ways. Three key distinctions merit clarification here: **Interfaces & Importance** (networks for people vs important Things vs everyday Things), **Performance Priorities** (network bandwidth vs latency and reliability), and **Network Architecture** (mobile vs stationary endpoints).

Interfaces & Importance: The Internet is generally considered the primary interface of human-oriented computing today. In contrast, the IoT will primarily facilitate machine-to-machine (M2M) computing between Things, rather than people. In other words, let us distinguish the Internet as being the Internet for People and the IoT as being the Internet for Machines.

For the IoT, we assert that some uses will be more important than others. This should affect the order, pace, and policies through which the IoT is developed and deployed. For example, certain critical services, such as electric power, telecommunications, military facilities, hospitals, public safety, and law enforcement should merit top priority. Key systems for commerce, such as data centers, roads, transit, and ports also stand out on the list. Consumer-facing services, such as smart appliances, will generate hype and seek attention but may end up most appropriately playing a supporting, rather than leading, role in the IoT.

Performance Priorities: Thanks largely to demand for streaming video, the Internet as we commonly know it prioritizes ever-increasing capacity for high-bandwidth content. In contrast, the IoT communications will be relatively low-bandwidth in comparison to the human-facing Internet. Although there is much hype around “big data”, the reality is that the vast majority of data generated by IoT devices is actually very modest in actual size, often smaller than a text message. (It is the value of the insights gleaned from analyzing patterns within large cumulative sets of numerous, albeit individually small, data points that is actually “big”.) Rather than solely emphasizing high bandwidth, the IoT also should prioritize low latency and high reliability to ensure timely and successful delivery of numerous, small data points to, from, and between IoT devices.

Network Architecture: From a network architecture perspective, the IoT will require innovations beyond traditional telecommunications approaches, in order to maximize access and deliver its full potential. As telecom has shifted away from providing regulated landline services and toward market-driven smartphone connectivity, we should recognize that mobile wireless solutions fall short of offering ubiquitous coverage. Consequently, there remain many underserved locations that are difficult to reach cost-effectively with landline and wireless telecom services. It is often just as, if not more, challenging to connect these areas with broadband Internet.

We assert that the IoT holds too many potentially transformative benefits for citizens and businesses to limit access to only easy-to-reach locations. Our experience has shown that it is cost-effective to leverage smart grid deployments that are well underway across our most widely distributed infrastructure - utility distribution grids - to serve as a foundation for extending IoT access as broadly as possible.

RECOMMENDATIONS

The IoT market is growing rapidly and organically as the costs of technologies fall and opportunities to modernize infrastructure emerge. Forward-thinking public policies can support and accelerate the emergence of IoT into the mainstream economy and our everyday lives. Toward this end, Silver Spring Networks proposes three areas for policy consideration regarding the Internet of Things: Spectrum, Security, and Access.

SPECTRUM: Ensure continued availability of unlicensed wireless spectrum for IoT in the US, and support efforts to encourage harmonization of this spectrum for IoT abroad.

Rapid market penetration of IoT devices and systems will require wireless spectrum for communications, particularly at the edge of IoT networks. There is growing industry consensus in the US around mesh networking technologies that utilize unlicensed band for last-mile communications through mesh networks to reach buildings. Because this particular spectrum is free, flexible, available, and effective (in terms of propagation characteristics for IoT communications), wireless mesh networking technologies can provide ubiquitous coverage cost-effectively and become enable IoT networks to become more, not less, robust as additional endpoints are added, in comparison to radial networks.

SSN proposes that the NTIA work to ensure that wireless spectrum remains free and unfettered by excessive use by specific devices or organizations. Existing rules have succeeded to date, but there have been, and will likely continue to be, commercial interests that seek to use more than their fair share of this spectrum.

SSN also requests support from the Federal government to make wireless spectrum more readily available in other countries for IoT utilization. Although market-driven industry standardization in IoT wireless spectrum standards is taking place to some degree, additional IoT-oriented wireless spectrum policy coordination between nations could bolster progress, accelerate deployment, and expand addressable markets for US IoT companies.

CYBERSECURITY: Invest in human capacity across industry and government to ensure cybersecurity for the IoT.

As context, SSN asserts that although there is some concern that networking critical infrastructure will increase vulnerability to cyber attack, the truth is that today's non-networked, largely analog systems are already highly vulnerable to large-scale, cascading catastrophes. With rigorous implementation, the IoT can maintain, and even improve, infrastructure security while also enhancing the resiliency and reliability of these systems to both natural and man-made challenges. As an example, the traditional power grid is susceptible to cascading blackouts under a wide number of scenarios. Applying IoT technologies to upgrade the analog grid to Smart Grid, however, can enable dynamic, self-healing capabilities that improve resilience and reliability, while also deploying defense-in-depth measures to manage and contain cybersecurity threats.

Getting IoT cybersecurity right will require significant investment in human capacity building for cybersecurity across industry and government. Vendors need deep expertise to develop and build secure technologies. Utilities, municipalities, and companies need the relevant skills and experience to choose systems wisely and implement them robustly. Governments at all levels – federal, state, and local – must acquire proficiency in evaluating and regulating the cybersecurity measures deployed by public and private entities over which they have jurisdiction. Across the board, we must invest in people to build technology proficiency, threat awareness, and protection vigilance.

SSN proposes federal investment in academic, professional, and vocational training to build cybersecurity human capacity in industry and government. In particular, state utility commissions would benefit greatly from federal assistance to develop relevant in-house expertise, facilitate the sharing of threat information and best-practices, and to promote intra- and inter-governmental coordination on cybersecurity issues.

ACCESS: Avoid creating an "IoT digital divide" by leveraging networked utility infrastructure to enable universal IoT access.

The IoT has the power to transform the way of life for everyone it reaches. Let us not inadvertently – or worse, intentionally – create an "IoT digital divide" by building these systems in a way that falls short of reaching all citizens and communities. Access to the IoT can be extended to virtually all citizens by leveraging our most universal infrastructure - the power grid - to serve as the foundational vector for IoT network deployment. Although grid modernization – the so-called Smart Grid – has gotten off to a successful start in the US, turning the Smart Grid into the foundation for the IoT will take innovative policies that enable and encourage utilities to open up their private Smart Grid networks to enable broader IoT access to non-utility participants.

CONCLUSION

Silver Spring Networks thanks the National Telecommunication and Information Administration for the opportunity to comment on this much-needed discussion on emerging IoT policy issues. We offer SSN's deep technical expertise and field-proven industry experience as a resource to NTIA on IoT topics going forward. We look forward to continuing to participate in this stakeholder dialogue and to turning the IoT's tremendous potential into a game-changing reality.