Afilias USA, Inc.
300 Welsh Road
Building 3, Suite 105
Horsham, PA 19044
T +1.215.706.5700
F +1.215.706.5701
W Afilias.info

13 March 2017

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Attn: Docket No. 170105023–7023–01
Washington, DC 20230

Re: Comments on "FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS"

Afilias welcomes the opportunity to contribute to the discussion of Internet of Things being led by the National Telecommunications and Information Administration ("NTIA"). The Internet of Things ("IoT") is a burgeoning market and it is important to ensure the fundamental building blocks are in place to create success. Afilias connects the world with reliable, secure, scalable and globally available technology that makes Internet addresses more accessible and useful. Afilias supports a wide range of applications, including domain registry services, Managed DNS, and Mobile and Web services. Based on these experiences, including developing and implementing security policy, we offer our responses to the green paper, "Fostering the advancement of the Internet of Things" organized by the questions posited in the Federal Register[1].

Q1: *Is our discussion of IoT presented in the green paper regarding the challenges, benefits, and potential role of government accurate and/or complete? Are there issues that we missed, or that we need to reconsider?*

NTIA should be commended on the scope of the green paper and the discussions, including the September IoT Workshop, completed to date. Given the vast marketplace that is covered by technologies with no consensus definition[2], NTIA has made a respectable effort to engage the appropriate voices throughout the technology sector from both service and policy vantage points.

The benefits of IoT will be realized with a definition of success that balances revenues, efficiencies, and intelligence with effective security and privacy protection. This statement is rooted in both an acknowledgement of the challenges facing IoT today and optimism that industry participants have a desire and tools to meet those challenges. Specifically, Afilias concurs the challenges include:

- Security. The creation and practice of protocols and solutions to protect our systems and data is paramount. We have already witnessed what happens when IoT is used against us, and it is critical to build security into every aspect of service delivery, and most critically at the infrastructure layer.

[1] Federal Register Notice Vol. 82, No. 9, Friday, January 13, 2017.

[2] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things,"January 2017, page 6.

- Interoperability. We agree with the need for deliberate and focused work to create new interoperability and communications standards. Specifically, this requires consensus on the operational standards around availability, e.g., deployment of standards, minimum response times, and service availability service level requirements.
- Privacy. We foresee the need for core principles around data management that reflect its value and ongoing and increasing threat of hacking. This framework is important to protect all data, both business and consumer data, which will also help guide important security protocols.
- Trust. There are several aspects of security to be considered and can generally be defined as ensure Trust. This involves a commitment to:
    - Global reach - IoT connectivity across networks and without geographic limitations;
    - Accessibility - device-agnostic connection; here, we will see the importance in IoT of adopting IPv6 and operational standards for connections;
    - Interoperability - an unwavering commitment to open standards. Afilias is a signatory to OpenStand[3], the modern paradigm for standards, shaped by adherence to five fundamental principles of Standards Development: due process, broad consensus, transparency, balance, and openness.
- Orphaned technologies. The 'things' we are connecting are not connected forever, and as such, introduce specific operational issues. This challenge is a hybrid of some challenges noted above and solutions to address planned and unplanned obsolescence must be defined in the early stages of development.

Consensus must be reached on each of these. We encourage the IoT sector to leverage proven, existing standards within the domain name system as valuable infrastructure resources, specifically in considering the use of the DNS and DNSSEC protocols.

With respect to a collaboration model, Afilias endorses a multistakeholder governance approach to IoT that allows industry to lead innovation and policy and invites government involvement as a participant. As an active member of ICANN, we can attest to the benefits of allowing industry room to innovate within a defined, fair and competitive structure. Relative to IoT, together, the private and public sector can establish a limited set of core principles and policies around technical standards, privacy and personal data and then create mechanisms for monitoring compliance.

This collaboration could happen ad hoc or as a part of a national strategy. While a national strategy could certainly unite industry in a clear path, we concur with other parties[4] that any strategy must not be overly proscriptive so as to allow the requisite flexibility to innovate. We agree NTIA should continue in the capacity of facilitator while the private sector leads the development of standards and interoperability. Further, we believe NTIA should be championing this multistakeholder approach through government and encourage other agencies exploring IoT regulations to adopt this collaborative, multistakeholder approach for engagement.

---

[3] see https://open-stand.org/

[4] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things,"January 2017, page 12.

Q2: *Is the approach for Departmental action to advance the Internet of Things comprehensive in the areas of engagement? Where does the approach need improvement?*

The four areas defined for engagement adequately cover the areas NTIA can plan their activities around fostering a secure and reliable IoT environment.

With respect to "crafting balanced policy and building coalitions", the green paper noted[5] the DDoS attack in October 2016 that highlighted existing vulnerabilities in devices and systems. It should be noted that this was not an inherent flaw in using DNS and should not be seen as an event that would give pause to using domain name-related systems and protocols. In fact, the domain names system has several benefits and features to be leveraged in many IoT applications. Firstly, there are existing security protocols such as DNSSEC to be utilized; these standards are proven and have been operational for nearly a decade. Secondly, the seamless scalability of the domain name system will prove ideal for IoT services requiring high levels of growth, and unique control over that growth. Thirdly, with service response rates in the milliseconds and zero DNS downtime, reliability is a built into the system. Additionally, DNS and registration systems consider data confidentiality as a core design element with flexibility to adapt to both new and evolving commercial and consumer models.

These are just a few things to consider in the " crafting balanced policy and building coalitions" and "promoting standards and technology advancement" areas of engagement. Afilias welcomes the opportunity to engage on these in more detail. Other groups to coordinate with this include the Internet Architecture Board (www.iab.org) and the Internet Engineering Task Force, "IETF" (www.ietf.org).

Q3: *Are there specific tasks that the Department should engage in that are not covered by the approach?* Focus on raising awareness of existing, proven technologies, and ensuring the emerging products and services take advantage of existing security technologies is a constructive activity for NTIA. Specifically, see comments above and below related to leveraging domain name-related protocols.

The domain name system can prove useful as IPv6 addresses are not human-friendly, whereas domain names are more relatable; and, it provides accountability of source data. Further, DNSSEC can address several IoT vulnerabilities:

- DNSSEC protects a user by ensuring the user knows exactly where to find whatever it is the user is looking for.
- DNS is a critical infrastructure system. Virtually everything depends on it.
- DNSSEC is the next step in the evolution of the Internet, similar to the web back in 1993.

Deploying a safe and secure DNS is not just the right thing to do, it is the cornerstone of building the next generation Internet, a safe and secure Internet and IoT environment.

Q4: *What should the next steps be for the Department in fostering the advancement of IoT?*

---

[5] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things,"January 2017, page 26.

There are two areas Afilias sees NTIA can be very helpful: nomenclature and facilitating the establishment of core principles within the industry.

NTIA can play an important role is in definitions and achieving a common language. While the risks of narrowness in defining IoT are real, Afilias believes there is an inherent importance to reaching common ground on definitions. In a keynote at ION Hangzhou[6], Afilias posited
"The Internet of Things is here, but there is no universally accepted definition, no single defined set of protocols. And this step — nomenclature — is an important step. Establishing the key terms and parameters now will help us proceed in a manner that focuses on what is important: secure, stable and reliable solutions from anywhere in the world.

The Internet Society tackled this last October. They define the Internet of Things ("IoT") as "the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered being computers." We at Afilias endorse this definition and framework. It recognizes that IoT is a broad landscape that covers several foundational communications technologies, protocols and user applications across various markets."

We encourage NTIA to consider the Internet Society definition[7]. In tandem, another framework to be considered is the Internet Architecture Board models for describing IoT interactions[8]:

1. Device to device – often have a direct relationship with built-in security and trust using device specific data models. Examples: Home automation systems like light bulbs, light switches, thermostats and door locks.
2. Device to cloud – often connects to an application service provider using existing communication (e.g., Wi-Fi) to extend the capabilities of the device. Examples: Enabling home energy consumption analysis and interactive voice recognition features.
3. Device to gateway – connects via application software operating on a local gateway device providing security and other functionality such as data or protocol translation"
    a. Popular with consumer items using an app on a smartphone to relay data like for fitness trackers;
    b. Useful for integration of legacy devices.
4. Back-end data sharing - a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. Extension of the device-to-cloud model that facilitates back-end data sharing, data portability and generally helps to break down traditional data silo barriers (still need common information models across vendors).

These models are a useful way of defining the interactions, their respective pain points and areas for future policy and standards development. Agreement on the key terminology will create a clearer environment for producing policy, standards and protocols.

---

[6] Delivered by Afilias CTO, Ram Mohan; transcript is available at:
http://www.circleid.com/posts/20160721_developing_internet_of_things_building_blocks/

[7] https://www.internetsociety.org/doc/iot-overview

[8] RFC 7452, "Architectural Considerations in Smart Object Networking" March 2015

Finally[9], we must accept the reality that the Internet advances at a rate that far exceeds any government's ability to keep up. Policy makers and regulators should focus on creating a framework that promotes security, privacy and accountability without setting limitations on innovation and growth. It is vital that industry and policy makers work in tandem to create a set of best practices based on a few core principles:

- Provide the greatest benefit to the user. The end user should be able to control the way they want to use a device — either for a single device or across numerous devices — and how they hide or share data. The user must be empowered to control all aspects.
- Focus on smart innovation, not creating boundaries or limits. Regulation that seeks to narrowly define, by definition will create boundaries on limitations and take the openness and out of the Internet.
- Make security and privacy a responsibility throughout the ecosystem: consider liability provisions that influence vendors to account for external third party costs created by insecure products or devices that create security or stability issues.

NTIA should play an active role here, and in creating fora for continued communication and information sharing.

[9] From Afilias ION keynote presentation, transcript at http://www.circleid.com/posts/20160721_developing_internet_of_things_building_blocks/