To: iotrfc2016@ntia.doc.gov
Subject: IAB comments on NTIA IOT RFC 2016
Date: Fri, 27 May 2016

Internet Architecture Board Comments to United States National Telecommunications and Information Administration Request for Comments, "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things."

The Internet Architecture Board is chartered with a responsibility to, among other things, "pay attention to important long-term issues in the Internet, and to make sure that these issues are brought to the attention of the group(s) that are in a position to address them. It is also expected to play a role in assuring that the people responsible for evolving the Internet and its technology are aware of the essential elements of the Internet architecture."(RFC 2850,"Charter of the Internet Architecture Board (IAB)," https://www.rfc-editor.org/rfc/rfc2850.txt)

In accordance with that role, we're pleased to be able to respond to the National Telecommunications and Information Administration request for comments on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things." [Docket No. 160331306–6306–01]

During the past ten years there has been a variety of IETF activities initiated to enable a wide range of Internet of Things devices to use interoperable technologies for communicating with each other. Today there are seven active working groups in this specific area, and of course many of the generic technologies developed in the IETF are also widely used in the Internet of Things. For more detailed information about the IETF's activities related to the Internet of Things, please see a recent article in the IETF Journal (https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf).

The IAB is also actively encouraging discussions across different standards developing organizations, consortia, etc. in the area of Internet of Things. The current activities in this area in the form of workshops are detailed in the specific responses below.

Our comments focus on the architectural and other technical elements of the questions offered, particularly with respect to the openness, scalability, and security of the Internet as it continues to expand to include "the Internet of

Things." It's our view that the questions raised can't be considered separately from the principles and considerations that have informed the Internet architecture to this point. The IAB would like to respond to the following questions posed in the NTIA request for comments:

Question 4: Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: Consumer vs. industrial; public vs. private; device-to-device vs. human interfacing.

Response: The IAB would like to draw the NTIA's attention to a recent document the IAB published entitled "Architectural Considerations in Smart Object Networking" (https://www.rfc-editor.org/info/rfc7452). Section 2 of that document includes a classification of four communication patterns common in IoT today, namely Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data Sharing. It also includes a discussion of a number of architectural issues that should be considered and hence the IAB believes such a classification, among others, should be used to improve the precision of technical and policy discussions.

Question 6: What technological issues may hinder the development of IoT, if any? a. Examples of possible technical issues could include: i. Interoperability ii. Insufficient/contradictory/proprietary standards/platforms iii. Spectrum availability and potential congestion/interference iv. Availability of network infrastructure v. Other b. What can the government do, if anything to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

Response: A number of technological issues that hinder the deployment of IoT are covered in Sections 3 through 5 of the aforementioned IAB document (RFC 7452). A significant problem that the IAB observed was the proliferation of competing standards for data models of various categories of IoT devices being done by many different organizations. Subsequently, the IAB organized a cross-organization workshop on IoT Semantic Interoperability (IOTSI) in March 2016 which included representatives of over 15 relevant IoT alliances and standards organizations, including NIST. A workshop report is in progress and will be published in the near future, but position papers from the various organizations can be found on the workshop website at https://www.iab.org/activities/workshops/iotsi/

Question 8: How will IoT place demands on existing infrastructure architectures, business models, or stability?

Response: RFC 7452 Section 3 recommends using existing protocols where possible, including the Internet Protocol (IP). The number of IoT devices is expected to be greater than the number of addresses available in IPv4. Only IPv6 will scale to the size expected for Internet communication.
The proliferation of multiple alternative protocols at every layer limits the interoperability between devices using competing standards.

Question 16: How should the government address or respond to cybersecurity concerns about IoT? a. What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns? b. How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

Response: Section 6 (Security Considerations) of RFC 7452 discusses a number of cybersecurity concerns that are unique to, or at least exacerbated by, IoT, and includes several IAB recommendations on this topic.

One of the key problems in many IoT environments is the inability to patch security issues in IoT devices. The IAB is organizing a workshop in June 2016 on IoT Software Update and will prepare a report afterwards. More information on this upcoming workshop can be found at https://www.iab.org/activities/workshops/iotsu/

With respect to how the government should address IoT security concerns, the IAB would like to reiterate its "Statement on the Trade in Security Technologies" (https://www.iab.org/documents/correspondence-reports-documents/2015-2/iab-statement-on-the-trade-in-security-technologies/); specifically the IAB recommends that restrictions on the international trade of security technologies be avoided. The IAB also would like to reaffirm the principle stated in its comments to the FCC (https://www.iab.org/documents/correspondence-reports-documents/2015-2/iab-comments-on-fcc-15-92/) that software security features must be broad enough to permit device firmware updates by parties other than the manufacturer itself.

Question 17: How should the government address or respond to privacy concerns about IoT? a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns? b. Do these concerns

change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)? c. What role or actions should the … government take…?

Response: Section 7 (Privacy Considerations) of RFC 7452 discusses a number of privacy concerns around IoT, and provides a number of IAB recommendations on this topic.

Furthermore, the IAB would like to draw attention to the IETF statement on pervasive monitoring, RFC 7258 (https://www.rfc-editor.org/info/rfc7258), for which the IAB has provided additional context in RFC 7624 (https://www.rfc-editor.org/info/rfc7624). Although these documents discuss privacy concerns around pervasive surveillance in general, as noted in RFC 7452, IoT devices often have even greater privacy concerns due to access to the user's physical environment and personal data.

Question 20: What factors should the Department consider in its international engagement in: a. Standards and specification organizations? b. Bilateral and multilateral engagement? c. Industry alliances? d. Other?

Response: The IAB endorses the OpenStand Principles for standards outlined at https://open-stand.org/about-us/principles/ and believes that adhering to such principles for IoT standards is essential in promoting a free and open Internet worldwide, promoting trust and confidence online, and promoting innovation in the digital economy, all of which the IAB notes are pillars defined by the Digital Economy Leadership Team (DELT).

There will be undeniable challenges to the evolution of the Internet as new kinds of devices connect and new patterns of use emerge. We thank the NTIA for its thoughtful questions, and hope that our initial answers are helpful to the NTIA in its deliberation. If you have additional questions for the IAB, please feel free to contact me.

Andrew Sullivan,
IAB Chair
For the IAB