Association for Automatic Identification and Mobility

May 23, 2016

National Telecommunications and Information Administration
US Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Attn: IOT RFC 2016
Washington, DC 20230

Re: **Initial Comments** of AIM, Inc. on:
Docket No. 160331306-6306-01 **RIN 0660-XC024**
Federal Register, Volume 81, Number 66, Pages 19956 – 19960. National Telecommunications and Information Administration, US Department of Commerce. *The Benefits, Challenges, and Potential Roles of the Government in Fostering the Advancement of the Internet of Things*.

To Whom It May Concern:

We are pleased to submit the enclosed comments regarding the above referenced docket and regulatory information number which appeared in Federal Register, Volume 81, Number 66, Pages 19956 – 19960.

These comments were prepared by members of AIM Inc, all of whom are subject matter experts of the design and application on automatic identification technology; specifically the Internet of Things. AIM, Inc. is a global industry trade association that represents the providers and users of technologies, systems, and services that capture, manage, and integrate accurate data into larger information systems that improve processes enterprise-wide.

AIM, Inc. strongly supports and commends the NTIA for its interest in the Internet of Things.

As subject matter experts in all automatic identification technologies, AIM Inc. will be happy to respond to any technical support requests from the NTIA.

Sincerely yours,

Chuck Evanhoe
AIM Board Chairman

20399 Route 19
Suite 203
Cranberry Twp., PA 16066 USA

Phone: +1 724 742 4470
Fax: +1 724 742 4476
email: info@aimglobal.org

General

1. The challenges are similar to those experienced during the Industrial Revolution of the 1800's and early 1900's; job obsolescence, job displacement, immediate job creation for which skill sets did not yet exist – or exist in depth, patent protection, training programs, and generally a "welcoming" environment. The opportunities are however much greater than anything we have seen before. The speed of change and the unbridled potential in near instant communication between heretofore disparate devices may well alter civilization in much the same way the printing press did.

1.a. Novel technological changes will occur as a result of the sheer amount of data and information created and transferred. New and different device technologies will emerge using longer range, lower power, and lower data rates than previously seen.

The need for standards will be greater than ever, but as the new technologies develop and applications emerge, the ability to write and maintain those standards will be incredibly difficult.

1.b. Novel approaches to policy development and change are already required. IoT growth is already on a steep upward curve and can be expected to go exponential in just a few years or less. Changes in technology and the application of that technology will happen faster than traditional policy development can react. Any lack of policy can result in widely divergent adoptions of technology, potentially denigrating of the US position as world leader in technology.

1.c. New opportunities are headed by the ability to accomplish so much more in so much less time using much fewer resources; The ability to have true "interconnectedness" with "things", without human intervention. The economic opportunities alone are staggering. What the economy has seen resulting from the Smart Phone culture will be a minor step when compared to what the IoT is capable of doing.

2. Each of the definitions of IoT so far has been a reflection of the author's perspective. Not surprising, the sensor industry defines the IoT as a collection of sensors. Telecommunications companies see it as a communication network. Each definition so far is limited by their view of the IoT horizon. All of these definitions are constantly evolving as new aspects of the IoT are identified. Combine this with the reality of

different agendas from other nations and a single definition of IoT may be just as elusive as the Holy Grail.

That said several international groups are grappling with this very topic. ISO/IEC JTC WG10 as a working group is dedicated to this endeavor as is the ITU-T. The best approach is to join these groups and use the internationally agreed definitions which will be by design slightly behind the development curve.

3. Existing personal privacy policies in the US exist. European policies are much stricter while Asian policies tend to be more lax. The existing policies give some protection, but the autonomous nature of the IoT will inevitably lead to vulnerabilities for both personal and corporate information. A single international approach to protection of data will be critical to ward off vast breeches of data.

4. Categorization of the IoT into horizontal groups as noted (public vs private etc.) is one necessary approach. Additionally, differentiation will also be required on a vertical basis i.e., Smart Cities, Smart Vehicles, Smart Hospital / Medical, etc.

5. Working Group 10 under ISO/IEC JTC1 is dedicated to the IoT and is developing a reference architecture, identifying gaps in standards coverage and building a vocabulary for use with the IoT. The reference architecture in particular is worthy of note. Built internationally it will serve as the backbone of the IoT development. AIM is directly involved with WG10 and has several members serving on it as both ad hoc Chairs and members.

6. In addition to the list provided security and privacy will be significant technological challenges for the IoT.

Government – private partnerships will be needed to keep policy development from lagging too far behind technology and application development.

7. Government technology activities will need to focus on

> RF spectrum utilization. How all of the existing RF technologies being implemented today interact with each other;
>
> Interoperability and non-interference. Keeping one technology from degrading the ability of any other;

Security and privacy. Especially with applications such as SMART Grid security or lack thereof can have a devastating impact on the population and the economy.

8. The IoT will stretch the existing infrastructure to a breaking point. With the unprecedented amount of data realized via the IoT, there will be pressure exerted to "do things" that the support systems will not be able to handle without change. Things like: Is the numbering schema used to uniquely identify "things" across the IoT adequate; Is there sufficient robust wireless connectivity; Which wireless system(s) to use and can the various different systems work together; Will legislation support expansion, or restrict it / curtail it.

9. Preparations for the IoT are currently spotty. Recommend immediate support of the expansion of a unique numbering schema that will work globally within the IoT. A global effort, such as that in ISO/IEC JTC1 will be required to work – "local" solutions won't last.

10. Major issues are things like internet neutrality and the interoperability/compatibility of the various technologies.

11. Measuring IoT as part of the digital economy is a good start. The services provided and commerce of digit goods should be included along with some measurement of the increase in data flow.

12. N/R

13. As the Industrial Revolution forever changed the face of America, the IoT will do the same – only more-so. Never before has so many people been able to affect so many different "things" BEFORE the IoT gets into full swing.

Once the IoT is instantiated to a greater degree than currently, you will see the streamlining of manufacturing processes to the extent that ONE "thing" could be made, and as competitively priced as current quantity pricing. Utilization of resources will become more efficient as there will be unprecedented visibility (and the ability to control any aspect within) all parts of the supply chain; this means less stock on-hand, quicker turns, the ability to change the order much later in the build process (greater customer satisfaction), more options offered to customer. This also means that the input side of the supply chain will be stressed as it isn't being now; smaller quantities required in quicker

time frames to potentially more places of manufacture – pushing the 3PL's and the transportation sector / infrastructure harder than is currently being done.

13.a. No Additional Comment

13.b. No Additional Comment

13.c. The Federal Government should exercise its powers to the extent that a minimum level of PROVEN cybersecurity is required, not just for the communications link but within IoT devices as well. Affected branches of the government should have a clear charter under OMB Circular 19 to seek out and participate in the development of voluntary consensus standards that underpin the IoT.

14. Changes in job classifications are inevitable, so training and education are a critical function of the government, especially for those that may be displaced from their job. Government will need to protect a manufacturing base in the USA not just for jobs but for defense and competitive necessity.

15. Data Security and Privacy. The introduction and spread of autonomous data generation and collection will place new meaning to the terms *security* and *privacy*. Corporate America will find requirements coming to them autonomously and will need assurances that the data is accurate. Financial institutions can deal with the fraud and identity theft questions, but simple things like the failure of a sensor in the refrigerator might fail to order milk, tempting a thief to think the homeowner was out of town and creating a dangerous situation during a subsequent break-in.

16.

16.a. The security concerns are much the same today as they will be tomorrow, but the impact will be orders of magnitude greater.

16.b. Clearly some data will require more security than others. That a family with small children routinely orders milk is of little consequence, and the supermarket today knows their buying pattern from their loyalty card. A computer manufacturer on the other hand, will want to keep their buying patterns between themselves and the supplier, not wanting their competition to know their sources and terms of sale.

16.c. No additional comment

17. The US needs to be aware of and responsive to privacy concerns at an international level. Companies and governments that deal internationally must provide privacy that meets the strictest requirements such as those in Europe today.

17a. Today privacy is pretty much protected by consumer consent. The consumer must make a choice. With the IoT the consumer may never know that their device is transmitting data about them autonomously. It is this autonomous data transmission, while not exactly new, will grow exponentially.

17b. The concerns do not change by category. Autonomous data transmission and collection is the problem across the board.

17c. Government actions to protect privacy need to be general enough to allow developers the freedom to innovate, yet comprehensive enough to require developers to actually provide consumers the ability to protect themselves.

18. Personal privacy is the name of the game. Opportunities for identity theft will grow as the number of autonomous transaction grows. Growth of the protection against identity theft industry is not a good thing in that it only means that identity theft is growing faster.

19. Poorer and disadvantaged groups can be both helped and hurt by the IoT

19a. The less advantaged people will find that the ability of their community to obtain social and governmental assistance will be improved. First responders will know more quickly about certain types of emergencies and be better able to respond.

19b. Just as the poorer communities will have greater access to services and goods, the ability of the more advantaged communities to pay for additional services and goods may well drain or strain the resources available to the poorer communities.

19c. Initially the internet will be one of the main highways for the IoT, it will explode in size / demand. The bandwidth requirements will not just arithmetically expand, but logarithmically. The real question is what will come after the internet to handle all the data that will be generated by the IoT.

19d. Fairness is a concept that often does not translate well into economics. Internet neutrality is an example of a good fairness concept. But fairness does not mean that every household gets the same size piece of pie. Communities on the other hand should be treated fairly with equal access.

20. Public Law already requires the adoption of voluntary consensus standards where they meet the requirement. Yet many state and federal agencies and departments do not participate in the development of those standards as specifically authorized by OMB Circular 19.

a. Specifically participation in ANSI, ISO/IEC and ITU committees must be expanded. Foreign nations are already attempting to dominate many of these committees developing IoT standards.

b. The European Union is already writing regional standards apart from the international standards bodies. Once in place the Vienna Agreement between ISO and the EU makes the adoption of those EU unique standards almost a given.

The US needs to apply pressure through ANSI to reduce the impact of the Vienna Agreement on the development of the IoT and the standards and rules governing its use.

c. Industry alliances and consortia should be encouraged to develop the IoT inside their own vertical. They have the most to gain and with a minimum of oversight should be better at developing the technologies and application than government.

21. Interoperability, both technically and operationally. Ensuring that there is international fairness and that the IoT is not forced to comply with the rules of the nation or region with the loudest voice.

22. The governance issues are the same. The big difference will be the magnitude of the impact.

23. No additional comment

24. The biggest issues for US companies will be restrictive rules on data transfer and financial matters. Of concern are rules that restrict foreign companies from doing business on an equal footing with domestic companies and those that restrict the access of consumers to the internet or IoT such as the “Great Firewall of China”.

25. Best way to handle this is to review those systems that have worked in similar environments and do the same thing / it in a similar way. Don't reinvent the wheel.

26. Participation in standards development at the national and international level. Avoid the mass meeting and data calls.

27. No Additional Comment

28. None at this time.