Before the
National Telecommunications and Information Administration
Washington, D.C.

In the Matter of	)	Docket No. 170105023-7023-01
	)	
The Request for Comments	)	82 Fed. Reg. 4313
On the Benefits, Challenges,	)	
and Potential Roles	)	
for the Government	)	
in Fostering the	)	
Advancement of	)	
The Internet-of-Things	)	

COMMENTS OF THE R STREET INSTITUTE

March 13, 2017

Prepared by:
Anne Hobson
Technology Policy Fellow
R Street Institute
1050 17th St NW #1150, Washington DC, 20036
202-525-5717
ahobson@rstreet.org

Introduction

On behalf of the R Street Institute, we respectfully submit these comments in response to the National Telecommunications and Information Administration (NTIA) request for comments on the benefits, challenges and potential roles for the government in fostering the advancement of the internet-of-things.[1] The R Street Institute is a free-market think tank with a pragmatic approach to public policy challenges.

We thank NTIA for the opportunity for further comment on this important emerging technology. The Department's green paper sets the appropriate tone by framing NTIA's role as one of support and encouragement of emerging technology.[2] While we will comment broadly on the role of the Department of Commerce ["Department"] in advancing a light-touch regulatory approach to the internet-of-things, our comments focus on our areas of expertise, including cybersecurity and user privacy. With this focus in mind, the below sections define the unique challenges and benefits the internet-of-things poses, outline the role for government (question 1), comment on areas of engagement (question 2) and detail how the Department should engage to advance the development of the internet-of-things (questions 3-4).

I. Benefits and Challenges in Internet-of-Things Development

As NTIA's green paper points out, the internet-of-things is challenging to define. Broadly, the "internet-of-things" is an array of connected objects with unique identifiers that have the ability to transfer data over a network.[3] These technologies have exciting applications in the fields of infrastructure, agriculture, energy, transportation, manufacturing, health and communications and more. According to McKinsey & Company, global internet-of-things adoption could generate between $3.9 and $11.1 trillion per year by 2025, equivalent to up to 11 percent of the global economy.[4] Internet-of-things devices can streamline routines and chores. They can leverage sensors and data to smooth traffic flows or signal when infrastructure need repairing. The combined scale, scope and interconnectivity can lead to economic growth and increases in productivity and prosperity. Yet, these features also present unique challenges.

---

[1] Department of Commerce, National Telecommunications and Information Administration, "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things," Request for Public Comment, Federal Register, Vol. 82, No. 9, January 13, 2017. https://www.ntia.doc.gov/files/ntia/publications/fr_iot_notice_rfc_01132017.pdf

[2] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[3] Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World," R Street Institute Policy Study No. 86, February, 2017. http://www.rstreet.org/policy-study/aligning-cybersecurity-incentives-in-an-interconnected-world/

[4] James Manyika, et al., "Unlocking the Potential of the Internet of Things," McKinsey Global Institute, June 2015. http://www.mckinsey.com/business-functions/digitalmckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physicalworld

Because of network effects, one device's vulnerability can become a problem for the entire network. Malware can infect vulnerable internet-of-things devices, form a botnet and organize distributed denial of service (DDoS) attacks to bombard websites or service providers with traffic. Such attacks can result in costly internet outages. The average DDoS attack can cost $500,000 for a firm.[5] Furthermore, the internet-of-things can be an avenue for physical attacks, cyber espionage, eavesdropping, data exfiltration or other attacks on our private data.[6] The consequences of device vulnerabilities are magnified by interconnectivity. Combating issues related to cybersecurity and privacy will require efforts from industry, policymakers, consumers and third parties. The Department can play a role in improving security outcomes by supporting market solutions and adopting a light-touch regulatory approach.

II. Role for Government

In addressing question 1,[7] we believe there is a role for the Department in supporting market-based mechanisms to addressing challenges in privacy and cybersecurity related to the internet-of-things. These market-based mechanisms should include private certification programs, industry-led information-sharing efforts, after-market solutions such as smart-routers and efforts to promote cyber-insurance adoption.

Health care, manufacturing, financial services, government and transportation were the top five industries that fell victim to cyber-attacks in 2015.[8] Some of these industries are more equipped to handle cyber risk. For example, the cyber-insurance take-up rate in the retail, health and financial services sectors is around 80 percent; however, less than 5 percent of the manufacturing sector has cyber-insurance coverage.[9] Cyber-insurance helps companies reflect on risks and plan for them and it aligns the incentives of insurers with the insured. Insurers perform risk assessments to ensure that the premium will cover the risk. Companies that demonstrate preparedness can get lower premiums.

The government is a high-profile cyber target with access to sensitive data about citizens. It is also a large buyer of internet-enabled devices. The Department can use this purchasing power to award contracts to internet-of-things contractors that emphasize data protection. It can also urge other federal entities to do the same.

---

[5] Incapsula, "Survey: What DDoS Attacks Really Cost Businesses," pp. 1-9, 2014. https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20 Impact%20Survey.pdf

[6] Mohamed Abomhara and Geir M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," Journal of Cyber Security, Vol. 4, pp. 65-88, May 22, 2015. http://riverpublishers.com/journal/journal_articles/ RP_Journal_2245-1439_414.pdf

[7] Question 1) 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?

[8] IBM X-Force Research, "IBM 2016 Cyber Security Intelligence," 2016. http://www-03.ibm.com/security/data-breach/cyber-security-index.html

[9] Council of Insurance Agents and Brokers, "cyber-insurance Market Watch Survey," October 2016. https://www.ciab.com/uploadedFiles/Resources/Cyber_ Survey/102016CyberSurvey_Final.pdf

One way to encourage cyber preparedness among contractors is to require contractors to demonstrate financial responsibility over the cyber risk they pose to the federal government. In this way, the Department can play a role in supporting broader adoption of cyber-insurance coverage to mitigate risks associated with cyberattacks. The Department can set an example as a market participant by signaling to industry that it is serious about encouraging cyber-insurance adoption to improve cybersecurity nationwide. Regulatory efforts that rely on market-based incentives such as cyber-insurance can have better, longer-lasting results than other legislative approaches.

We commend NTIA for following the approach detailed in the 1997 Framework for Global Electronic Commerce.[10] This framework reinforces the importance of industry-led policies and defines government's role as fostering that development. In the green paper, NTIA recognizes the danger of inconsistent or unpredictable regulation and acknowledges the importance of letting companies experiment.[11] Promoting an open global environment for internet-of-things development is key to realizing the benefits of this technology.

As this technology matures, the Department should pursue a light-touch regulatory approach to the internet-of-things. Because devices are diverse in functionality and nature, one-size-fits-all regulation based on design standards is bound to have deleterious effects. Design requirements risk being overly complex or inadequate and would be difficult to change over time once they are applied. Moreover, compliance costs with such requirements could deter internet-of-things innovation. Lastly, such requirements would crowd out private efforts to improve cybersecurity and privacy at the industry and firm level.

Any requirements should be as narrowly focused as possible and should emphasize performance standards rather than design standards. Performance standards specify the desired outcome of a policy while allowing companies the flexibility to identify the best means or design to achieve it.[12] By contrast, design standards specify the manner in which the outcome is achieved. NTIA should refrain from constructing restrictive regulatory regimes, while seeking out ways to encourage firms to share threat information, promote cyber-insurance adoption, encourage private efforts to recognize security-conscious products with certifications, develop and adopt best practices voluntarily and reward innovative after-market approaches to policy issues such as cybersecurity and privacy.

The internet-of-things is a complex system. There is no simple regulatory fix. Instead, industry, governments, consumers and third party stakeholders will have to work together to improve security and privacy outcomes. NTIA should continue to play the role of convening stakeholders and encouraging discussion around issue areas such as cybersecurity and privacy.

---

[10] The Framework for Global Electronic Commerce (July 1997), https://clinton4.nara.gov/WH/New/Commerce/.

[11] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017, page 14. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[12] David Hemenway, "Performance vs Design Standards," U.S. Department of Commerce, NIST, pp. 1-35, October 1980. http://gsi.nist.gov/global/docs/pubs/NISTGCR_80-287.pdf

III. Areas of Engagement and Next Steps

The approach detailed for departmental action includes appropriate areas of engagement; however, to address questions 2 and 3,[13] there are specific opportunities for engagement that should be included. For example, the green paper argues the Department can play a role in encouraging risk-based approaches. One of these risk-based approaches should be promoting cyber-insurance adoption. The Department can encourage cyber-insurance adoption and risk mitigation among the vendors with whom it contracts.

In the section "Proposed Next Steps," NTIA suggests the Department can "leverage its role as an internet-of-things consumer to promote a market for secure internet-of-things technologies and the supply chains supporting those technologies."[14] In answer to question 4,[15] we propose the Department can achieve this goal by introducing a financial responsibility requirement in its contracts with internet-of-things device vendors to transfer the financial and operational risks of cyber-attacks. This will help companies recover and prevent high vendor turnover due to a cyberattack. It will promote cyber-insurance adoption more broadly, helping to immunize the entire internet-of-things ecosystem from cyberattacks. Moreover, it will encourage market growth for risk-based products and increase the availability and affordability of insurance products. Such an approach would signal to industry that the Department is serious about bolstering the nation's cyber preparedness in light of the unique challenge posed by the internet-of-things.

Conclusion

We are encouraged by NTIA's efforts so far to understand the internet-of-things, engage stakeholders and develop a constructive policy approach. There is a role for the Department of Commerce to support market-based solutions to cybersecurity and privacy concerns related to the internet-of-things. We look forward to continuing to engage with the Department on this topic.

Respectfully submitted,
Anne Hobson
Technology Policy Fellow
R Street Institute

---

[13] Question 2) Is the approach for Departmental action to advance the internet-of-things comprehensive in the areas of engagement? Where does the approach need improvement?
Question 3) Are there specific tasks that the Department should engage in that are not covered by the approach?

[14] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017, page 54.
https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[15] Question 4) What should the next steps be for the Department in fostering the advancement of IoT?