SIIA Accelerating Innovation in Technology, Data & Media

202.289.7442 1090 Vermont Ave NW Sixth Floor
www.siia.net Washington DC 20005-4905

March 13, 2017

Travis Hall
National Telecommunications and
Information Administration
U.S. Department of Commerce,
1401 Constitution Avenue NW., Room 4725
Washington, DC 20230

Dear Mr. Hall,

On behalf of the Software & Information Industry Association (SIIA), thank you for the opportunity to respond to the National Telecommunications and Information Administration's (NTIA) green paper, *Fostering the Advancement of the Internet of Things.* SIIA appreciates the in-depth technical and policy analysis presented in this paper, and we commend NTIA staff for working collaboratively throughout this process.

SIIA is the principal trade association for the software and digital information industries. The more than 700 software companies, data and analytics firms, information service companies, and digital publishers that make up our membership serve nearly every segment of society, including business, education, government, healthcare and consumers. As leaders in the global market for software and information products and services, they are drivers of innovation and economic strength. SIIA member companies provide critical data and analytic services that power the Internet of Things (IoT).

SIIA concurs with the premise of this paper that infrastructure and policies are critical to enabling the full potential of the IoT. We also agree that the Department of Commerce (Department), and particularly the NTIA, is well suited to assess these issues and to champion the Administration's efforts towards the development of a robust IoT environment that benefits consumers, the economy and the Nation as a whole.

We are pleased that the paper reflects the Department's agreement with many of our key conclusions and policy recommendations. As we highlighted in our comments, overarching policies and regulations would stifle innovation and growth. The Paper reflects the broad agreement that policymakers should rely heavily on the current framework which is sufficiently flexible to promote exciting new IoT innovations and enable the transformative benefits of the IoT that promise to fundamentally improve the way business is done and the way people live.

SIIA also concurs with the Paper's identification of key issues that can impact the deployment of IoT technologies, the wide-scale benefits and lingering challenges. As the Department continues to assess what role, if any the U.S. Government plays, and particularly the Department, we offer the following responses to the Paper's recommendations, *Crafting Balanced Policy and Building Coalitions,* for proposed next steps.

The IoT is already visible across many facets of everyday life, from industrial uses, to education, smart cities and enhanced government, transportation and personal aspects, including wearables, domestic appliances and our automobiles. The issues surrounding the IoT are just beginning to be framed for public debate. The IoT is developing healthily in the presence of many well-understood legal doctrines that protect health, safety and property rights.

More often than not, existing laws are continuing to function quite effectively and provide substantial consumer protection, even in light of rapid technological innovation over the last decade—again many of the issues associated with the IoT have been debated for many years as relevant to the rise of "big data." For instance, the current U.S. sectoral approach to privacy and security serve as excellent examples of how policies can effectively protect consumers without taking a comprehensive, one-size-fits-all approach. Under the current approach, security, responsibility and accountability for data are commensurate with the associated risk. This approach is absolutely critical as we move further towards an "Internet of Everything" environment with such a diverse set of applications across so many different sectors of the economy and facets of our lives.

Of course, there are challenges presented by the IoT. While many of these challenges are not entirely new, they could pose significant impediments if there are gaps in the current policy framework that lead to harmful results for consumers and citizens. As we noted in our previous comments, SIIA's preeminent policy recommendation is that given the complexity of the IoT, with myriad different devices, platforms and inter-related technologies, there is no overarching policy or singular framework that could be expected to effectively apply across the board.

SIIA has long been a supporter of the NTIA multistakeholder efforts to create voluntary codes of conduct and best practices in the areas of privacy and cybersecurity, with the goal for a flexible IoT policy framework, rather than a prescriptive approach, where innovation can continue to thrive, but where regulations can provide a backstop to prevent significant harm. We have been a leading participant throughout these initiatives, and we believe that the dialogue among diverse stakeholders, and the outcomes of these processes, have largely helped to shape policy debates across a wide spectrum of privacy and security issues. We encourage the Department to continue utilizing these processes with respect to IoT policies.

Similarly, the NIST Cybersecurity Framework provides an excellent example of the valuable role for government, particularly the Department and NIST, in convening stakeholders to develop a flexible, risk-based security framework. Notably, the ongoing effort to update this Framework demonstrates the need for these frameworks and policies to evolve with technology and to be improved based on implementation and user experience. SIIA strongly encourages the Department to support NIST's continued leadership in the governance of the Cybersecurity Framework, and their leadership in sharing of information, practices, and industry resources.

While we agree largely with the recommendations laid out in the paper, and we greatly value the Department's leadership efforts in helping to craft key policies and promote public-private collaboration, we disagree with respect to the recommendations pertaining to privacy. Specifically, SIIA disagrees with the Paper's recommendation for the Department to continue supporting baseline privacy legislation. Rather, SIIA believes that American consumers are already well served by U.S. privacy laws and regulations, as well as voluntary industry initiatives, which provide for strong safeguards and accountability to protect consumer privacy. SIIA believes that the current sectoral approach to privacy, focusing on sensitive data pertaining to health, finance, eligibility and children's privacy is well suited for the IoT. Any gaps identified down the line are likely best addressed narrowly, rather than through a new comprehensive privacy framework. We also promote the continued use of organizational policies governing information collection, management and use that provide for responsible data management, satisfy legal requirements and retain the flexibility to meet evolving social norms and cultural expectations surrounding the IoT.

With respect to the recommendation to provide for an engineering approach to privacy, we are not clear how the Department proposes to enable this, and what the outcome might be. SIIA and a coalition of companies engaged with the department between 2014-2016, regarding efforts underway within NIST to advance privacy engineering. In 2014 and 2015 we expressed concerns to NIST about the direction of its proposed Privacy Engineering initiative[1] and in 2015 we engaged with continued concerns about the draft NIST policy guidance regarding privacy engineering.[2]

SIIA agrees that there is significant value in the collaborative work between NIST and industry in this area, but the status and continued objectives of the Department are unclear at this time. SIIA looks forward to more clarification from the Department about what activities may be contemplated in the future, particularly with respect to the IoT. We look forward to continued collaboration between industry and the Department to achieve common objectives around privacy and security engineering.

Again, thank you for the opportunity to comment in the early stages of this policy assessment, and on this Green Paper.   We encourage continued engagement by the Department, and we look forward to working together, to ensure that the United States does all that it can to promote full development, and the full benefits of, the Internet of Things.

Sincerely,

Ken Wasch

Ken Wasch
President

[1] http://www.siia.net/Portals/0/pdf/Policy/Privacy%20and%20Data%20Security/industry_letter_to_nist_re_privacy_engineering.pdf?ver=2015-03-26-132909-097

[2] http://www.siia.net/Portals/0/pdf/Policy/Privacy%20and%20Data%20Security/MultiAssociationSubmissionNIST%20July30.pdf?ver=2015-07-30-134039-967