SIIA Accelerating Innovation in
Technology, Data & Media

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

May 27, 2015

Mr. Allan Friedman
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

RE: Request for Comment, Stakeholder Engagement on Cybersecurity in the Digital Ecosystem [Docket No. 150312253–5253–01]

Dear Mr. Friedman,

On behalf of the members of the Software & Information Industry Association (SIIA), thank you for the opportunity to provide comments in response to the Department of Commerce (DOC) Internet Policy Task Force's (IPTF) request for comments to identify substantive cybersecurity issues that affect the digital ecosystem and digital economic growth. SIIA welcomes the opportunity to help achieve broad consensus and coordinated action towards the development of voluntary best practices and policy guidelines to improve security for organizations and consumers.

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—software alone contributes $425 billion to the U.S. economy and directly employs 2.5 million workers and supports millions of other jobs. For more information, visit the SIIA Policy Home Page.

SIIA and its members share the Administration's critical priority to enhance the cybersecurity of our Nation. We are dedicated to maintaining and expanding the partnership between the private sector and the government to address our collective cybersecurity challenges. To that end, we have spent much time over the last several years working closely with Administration officials and Congressional leaders to develop policies to address increasing cybersecurity challenges.

SIIA has long been supportive of a flexible, voluntary approach to developing cybersecurity best practices, consistent with the efforts identified by the Administration’s 2011 Green Paper, and the recent NIST Cybersecurity Framework. In contrast, a regulatory approach is not well suited to address rapidly-evolving cybersecurity threats, because it does not provide for the reality that different entities face different challenges and threat levels. Additionally, solutions to cybersecurity must remain technology neutral, rather than promoting various technologies or platforms over others—security policies must avoid picking technological winners and losers.

SIIA strongly concurs with the NTIA’s objective to enhance stakeholder engagement on cybersecurity, particularly the notion that development and promotion of voluntary policy guidelines, procedures and best practices could substantially improve cybersecurity for both organizations and consumers across a number of key areas where challenges are greatest.

Of course, in some areas, much work has already been performed to develop and refine best practices, where others not. While SIIA agrees that NTIA should avoid duplicating existing work, we support NTIA’s efforts in this process to evaluate both those areas where voluntary practices, guidelines and initiatives are already available and could use the benefit of broader promotion and adoption, as well as areas where it would be useful to convene experts and stakeholders to develop new voluntary guidelines or best practices.

SIIA also strongly concurs with the objective to focus on a narrow, definable area where consensus can be reached in a reasonable timeframe and substantial benefit can be achieved. To this end, and consistent with the goal to address issues affecting the digital ecosystem as a whole, and promoting the digital economy, we offer the following feedback regarding possible topics for consideration.

I. Key Issues for Consideration

As you know, modern cyberattacks are not simple, isolated events. Rather, attacks frequently begin by establishing a foothold within an infrastructure, often at an endpoint using malware and establishing botnets for collecting confidential information or launching complex attacks to compromise other networks and steal valuable information and intellectual property. Once an endpoint is compromised, the attacker can move laterally to find and exploit other systems until the attackers locate the data, credentials or processes they are seeking.

Despite significant security practices by most companies and many consumers, vulnerabilities are increasingly exploited by online fraudsters, leading to identity theft and cyber fraud, causing material harm for consumers and businesses across a wide range of industries (including retail, banking and financial services, tax, etc.). Advanced cyber attackers have the advantage – they only need to exploit a single vulnerability, while organizations must protect every system and vector, including all of their employees and customers.   Individuals and businesses are continually seeking to better detect, analyze, prevent, and respond to these advanced and continually evolving threats. Unfortunately, this is an increasingly challenging battle for U.S. businesses, particularly for small and medium-sized businesses lacking substantial cybersecurity expertise and resources.

In light of this current reality, SIIA has identified three areas where there is a significant need to effectively define cybersecurity gaps and advance best practices, with a particular focus on informing and helping to protect the cybersecurity readiness of small and medium-sized entities, and end users. For the reasons outlined below, SIIA urges NTIA to focus its efforts in part on further advancing the various best practices for stronger authentication protocols that could keep customer data out of the hands of cyber-criminals and stem the tide of identity theft, as well as further awareness, consensus and best practices around botnet and malware mitigation.

1. Internet Authentication – At a time when Americans are performing increasingly important functions online—including managing bank accounts, shopping, paying bills and handling medical records—it is imperative that our collective cybersecurity focus includes efforts to help protect the most vulnerable: consumers who can easily fall victim to attacks that leave personal data vulnerable to hackers and cyber-criminals. Once a consumer's data is compromised, it can then be used to wreak havoc, including identity theft, take-over of online accounts, and to commit fraud. In many cases, the end result is considerable financial harm to the consumer, and sometimes the entity providing the service.

Fortunately, there has been much work performed around improving authentication. Notably, the The FIDO (Fast IDentity Online) Alliance, a non-profit organization formed in 2012 to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords, has gained strong support and participation from the a cross-section of technology companies in an effort to develop specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. The Alliance has produced multiple specifications that serve as examples of the work where a multistakeholder initiative could possibly further add credibility and consensus around critical practices to enhance authentication.

SIIA recommends that NTIA consider this and other initiatives where there is broad consensus with the goal of engaging a broad group of stakeholders to change the nature of authentication, bringing it into the 21st Century.

2. Botnet Mitigation – The software industry is at the forefront of the fight against botnets and other forms of Internet security threats, including notification efforts for users of computers and routers infected, and in the provision of tools for consumers and businesses to keep their systems free of infections and to remove malware and botnets from their infected systems.

SIIA is committed to addressing botnet security threats by working collaboratively with the government and by promoting the work of our members. We participated in the DOC-led Industry Botnet Group ("IBG"), a multistakeholder process convened in 2011 which produced Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace. These Principles were a positive step forward, calling on Internet participants to coordinate and communicate with each other and voluntarily work to fight the effectiveness of botnets across the botnet lifecycle. However, there is much work still to be done, as botnets remain a major challenge to our Nation's cybersecurity and digital commerce, continuing to infect computers, threatening the trust and confidence of online users and undermining the efficiencies and economic growth spurred by the Internet. Industry and government must continue to work together to further combat these challenges, and NTIA's involvement could provide a valuable coordinating function at this time.

3. Malware Mitigation/Malvertising – Malware is a closely-associated cyber threat, often serving as the root cause of botnets. SIIA therefore also supports the NTIA focus on the growing threat of malware and specific strategies to mitigate malware. In 2012, the U.S. Computer Emergency Readiness Team (US-CERT) produced a paper to inform organizations of this rapidly growing problem and provide best-practice defense tactics. US-CERT identified that malware has advanced from mere disrupting services to well organized schemes actively seeking financial gain. Attackers using malware have become adept at circumventing traditional defenses such as anti-virus software and firewalls. Even encrypted web transactions may not protect sensitive information if the user's computer has been infected.

Malware remains one of the greatest cybersecurity challenges to consumers and businesses, particularly small and medium-sized businesses with fewer resources to protect themselves. Not only are there the challenges associated with protecting systems from malware, but once a system is compromised, organizations need to improve the ability to minimize their damage. Because today's malware uses multiple vectors to spread including infecting file shares and brute-forcing weak passwords, organizations need to implement comprehensive information security policies and procedures that address all areas of potential compromise and vectors of attack.

SIIA believes that much additional work could be done focusing on voluntary guidelines, procedures and best practices to combat the threat posed by malware and "malvertising."

II. Areas where we believe NTIA should proceed with caution:

1. Internet of Things – The emerging Internet-enabled IT ecosystem, or the Internet of Things (IoT), has already spurred tremendous opportunities for social innovation and economic growth, and it is only still in the initial stages. Recognizing that data-driven innovation is at the core of these vast benefits, and that this sometimes involves personal or sensitive data, there are no doubt security challenges presented by the IoT. However, IoT is comprised of so many different technologies, platforms and devices, that it would not be productive to initiate multistakeholder efforts around IoT cybersecurity, writ large. That said, to the extent it is possible to identify various elements of the emerging IoT universe where collaboration could seek to identify and accelerate best practices, SIIA would support those efforts.

2. Privacy – SIIA has been a strong supporter of NTIA's privacy multistakeholder initiatives—we were a leading participant in support of the Mobile Transparency Code of Conduct produced by the first initiative, and we are actively engaged in the second initiative on facial recognition. Much like cybersecurity, this is an area where we believe that a multistakeholder process to develop voluntary codes of conduct and best practices is superior to a regulatory approach.

SIIA recognizes that privacy and cybersecurity are intrinsically linked because the security of personal information is a critical component of various effective cybersecurity frameworks. While we strongly support multistakeholder initiatives focused on authentication techniques, voluntary policies and practices to prevent fraud and identity theft,, we do not believe it would be productive to focus cybersecurity multistakeholder discussions on practices to promote privacy, broadly. To the extent privacy issues are discussed within various cybersecurity discussions, we think they can be done in a complimentary manner.

III. Recommendations on Implementing the Multistakeholder process

SIIA strongly supports NTIA's goals to ensure openness, transparency and consensus-building as fundamental pillars of cybersecurity multistakeholder processes. These are critical elements to maximize the efficiency and effectiveness of the overall process. To help achieve these goals, SIIA recommends that NTIA develop public inclusive mailing lists that extend beyond the participants in a working group to maximize public discussion of the multistakeholder process, rather than merely communicating within a set group established at the early stages. Specifically, SIIA supports the use of GitHub for gathering public input, consistent with the approach that was used by the Administration's gather of public comments on the HTTPS-only gov sites policy.

Also, given that the various topics considered have critical elements ranging from very technical practices and specifications to high-level policy recommendations, SIIA encourages NTIA to help stakeholders engage at a level where they are best suited to contribute positively.

IV. Conclusion

Again, thank you for the opportunity to provide input on this very important process. On behalf of our members and industry, SIIA looks forward to working closely with you to initiate this worthwhile objective and begin developing helpful guidance and codes of conduct to enhance our Nation's collective cybersecurity. If you have further questions or would like to discuss, please contact David LeDuc, SIIA Senior Director for Public Policy, at dleduc@siia.net or 202-789-4443.

Sincerely,

Ken Wasch

Ken Wasch
President