The Computing Technology Industry Association
Docket No.: 150312253-5253-01
The Department of Commerce Internet Policy Task Force
National Telecommunications & Information Administration

On behalf of CompTIA, thank you for the opportunity to provide comments on cybersecurity issues that affect the digital ecosystem and digital economic growth. This is an issue that we have followed closely over the last several years and have actively engaged with the Department of Commerce on.

As you may know, CompTIA is a nonprofit trade association representing more than 2000 member companies. Our members include computer hardware manufacturers, software publishers, and a large number of small and medium sized IT service providers, as well as the distribution partners that bring these products and services to market.

CompTIA is also the leading provider of vendor neutral IT workforce certifications. We believe that industry recognized certifications play a critical role in our national and economic security. Those responsible for hiring the best human talent must have confidence – before a breach or breakdown occurs - that employees are trained and equipped in a manner that can be identified, measured, and validated.

Our comments revolve around one major premise: trust. The threat landscape is rapidly changing, as are the technologies and best practices that we use to combat the threat. Mutual trust and collaboration within industry and between government and industry is critical in order to effectively address various threat actors. We believe NTIA has an important role to play in helping to foster a trusting relationship. A climate of trust will help to facilitate greater information sharing and collaboration. In particular, the ecosystem would benefit greatly if there was enhanced sharing of threat intelligence, data breach experiences and best practices.

Foreign nation states and other threat groups, wishing to destroy, disrupt and steal sensitive information in order to do harm to U.S. interests, are constantly attacking both government and civilian systems. Data breaches are on the rise without any sign of slowing down. According to Verizon's 2015 Data Breach Investigations Report, there were 79,790 "security incidents" in 2014 and 2122 "confirmed data breaches," both all-time highs[1]. Further, roughly two-thirds of those incidents occurred in the U.S. Cyber criminals are becoming increasingly sophisticated and companies simply cannot keep up on their own.

Both the private sector and government possess valuable intelligence regarding a wide range of threats, which, if shared, would allow for both parties to identify trends and more-effectively protect against these threats before they have the opportunity to breach our digital infrastructures. Further, threat intelligence is key to the effective detection of and response to attacks.

The sharing of information between companies would slow these criminals down significantly and provide an early warning system regarding new and evolving threats. Cyber criminals often do not stop after attacking just one company, and often try to capitalize quickly once they've found a successful method. In fact, 75% of cyber

---

[1] Verizon 2015 Data Breach Investigations Report, P. 1, *available at* http://www.verizonenterprise.com/DBIR/2015/

attackers hit a second victim within 24 hours of their first attack, and 40% attack that second victim within an hour[2]. If companies had a better way to share information about these attacks with one another, they could communicate threats quickly and alert other companies about how these attacks have been carried out. This would help companies protect themselves against new and ever-changing types of cyber attacks.

Threat intelligence has become a valuable commodity in the private sector, resulting in the emergence of lucrative business opportunities to collect, analyze and sell threat intelligence as a service. The high value attached to commercial cyber threat intelligence and high-costs needed to provide it, with both quality and at scale, have left the private sector with little incentive to share this information with the government. In addition, concerns regarding potential liabilities for the organizations sharing threat intelligence with the government remain and add to the private sector's reluctance to share.

At the same time, the government is broadly perceived to lack the ability or willingness to share information of similar value. This industry perception exists not from the belief that the government lacks threat intelligence, but rather due to the historically poor information sharing between state and federal agencies and an over-classification of information. Furthermore, there are concerns and some confusion as to whether or not U.S. legal precepts have kept pace with modern data sharing, and if doing so is legal and able to remain confidential. In addition there is concern that interpretations of "business confidential information" can vary, resulting in sensitive information shared with the government being made publicly available.

CompTIA believes this problem can be directly addressed by improving upon the existing government and private sector partnership. For example, a specific focus on identifying value in both a party's data and technical mechanisms will enable the bilateral sharing of this information in a timely manner, and in doing so will create an atmosphere of trust. In recent years, Congress has struggled with passing meaningful legislation to help facilitate these changes. Although CompTIA is supportive of The National Cybersecurity Protection Advancement Act (H.R. 1731) and the Protecting Cyber Networks Act (H.R. 1560), both of which have passed the House of Representatives with bipartisan support, we cannot afford to wait for these bills to become law before instituting change. Legislation, if and when it is signed into law, will be a critical piece in helping to reinforce and compliment collaboration that is already underway.

Unfortunately, companies are hesitant to share information with one another for fear of that information becoming public and harming their reputations. Most state laws only require companies to disclose breaches publicly if potentially harmful information has been acquired, but most of the "security incidents" mentioned above would not trigger notification. Companies want to avoid alarming customers over incidents that pose no risk to customer information.

However, sharing information about these security incidents with the broader

---

[2] Verizon 2015 Data Breach Investigations Report, P. 11, *available at* http://www.verizonenterprise.com/DBIR/2015/

business community could help other companies protect their information and lead to stronger security nationwide. In particular, the small and medium business (SMB) community would benefit from this information sharing, and the inclusion of best practices on how to address such breaches, because they simply do not have the same resources as large companies to put towards security measures.

CompTIA also recommends continuing the workshops and roundtables on the NIST cybersecurity framework. We believe that continued conversation on the framework will help to create trust through the sharing of best practices and experiences on both the government and industry side. Continuing these workshops will also aid in identifying gaps that need to be addressed within the framework. The underlying premise is that the public-private sector partnership must be continuous when it comes to cybersecurity, as opposed to starting anew again and again.

Additionally, the SMB community must be better integrated into these processes. Depending on the definition used, the number of SMBs that own or operate critical infrastructure ranges from 4,620 to 13,861[3]. The SMBs play a crucial role in our national and economic security and are often left out of the conversation. We recommend engaging with the Small Business Administration (SBA), an entity already known to many of the SMBs, to ensure that companies of all sizes are creating trust with the government. Very often these companies partner with larger organizations, and the sense of trust must be felt throughout the chain in order to be effective.

We want to thank the NTIA for taking the lead on such an important issue. As a part of the DOC, it stands within an agency that has worked diligently to ensure that the concerns and needs of industry are heard. We look forward to continuing to work with the agency on this difficult yet critically important issue.

[3] U.S. Economic Census, 2010