CompTIA

The Computing Technology Industry Association
Docket No.: 151103999-5999-01
National Institute of Standards and Technology
Request for Information on the "Framework for Improving Critical Infrastructure Cybersecurity"

515 2nd St., N.E. Washington, DC 20002

On behalf of the Computing Technology Industry Association (CompTIA), thank you for the opportunity to provide comments to NIST on "Views On the Framework for Improving Critical Infrastructure Cybersecurity." CompTIA has been an active participant in the creation and implementation of the framework. We look forward to continuing our dialogue and appreciate the opportunity to remain engaged during this next phase of framework improvement.

The Computing Technology Industry Association (CompTIA) is the voice of the information technology industry. With approximately 2,000 member companies, 3,000 academic and training partners and nearly 2 million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications and public policy advocacy. Through its advocacy arm, CompTIA champions member-driven business and IT priorities that impact all information technology companies – from small-managed solutions providers and software developers to large equipment manufacturers and communications service providers.

We would like to thank NIST for its efforts on the Framework thus far. First and foremost, we are most appreciative for NIST's commitment in engaging the private sector in forming and updating the Framework. Your commitment to this process is to be applauded. We would also like to commend you for the success of the Framework thus far. We know that many organizations in our industry and within our own membership have embraced the Framework, and in doing so, have strengthened their own cybersecurity.

Our comments for improvement are focused on two key areas: training and awareness of personnel and the ability for the small and medium sized businesses (SMBs) to utilize the framework. Both of these areas are a top priority for us as an organization and we appreciate the opportunity to share our expertise.

According to the 2015 CompTIA "Trends in Information Security" study, human error accounts for 52% of the root case of security breaches. This human error can be caused by anyone, not just personnel and partners with information security-related duties. Given this risk, we were pleased to see the Framework include a training and awareness section in its first iteration. As it currently stands, this section reads: "The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. While this was an important first step, CompTIA believes that this should go further. We suggest that the training and awareness section reflect the reality that any person with access to an organization's computer system has a role to play in ensuring its cybersecurity by updating the definition and the tiers. We encourage all employees to have some level of cybersecurity training and believe that the framework should reflect this as well.

Further, there is little information on what constitutes training. We recommend that

guidelines be provided so that organizations that have had little to no experience with training can, at the very least, have a starting point. This is especially helpful for the SMB community that may not have the background knowledge and very often the resources needed, to vet various training options. We are aware that NIST will not and should not pick specific training vendors to recommend. Instead, we suggest including a listing of topics that should be covered by training for the various tier levels. An example of this is the Department of Homeland Securities National Initiative for Cybersecurity Careers and Studies (NICCS) portal. While not endorsing any one certifying body or training organization, this map provides insight for what skills are needed, and how they can be ascertained, for particular cybersecurity jobs. It is likely that NIST could leverage components of the NICCS portal for this update.

Furthermore, by using the NICCS portal as an explicit reference, it will enable framework users to have a better sense of what their personnel in similar job roles should be trained and certified to do. It is also important that the various frameworks that have been put forward by government to heighten our cybersecurity serve as complimentary components of each other, and this will certainly help to further that goal.

Regarding the SMB community, we applaud the specific outreach that has taken place with this segment of the critical infrastructure population. However, we urge that NIST specifically target this community for their input before updating the framework. An RFI, despite being publicly posted, is something that very often will not fall on the radar of those located outside the beltway. We suggest reaching out to state and regional technology councils for their help in facilitating outreach with their members and participants. Through our partnership with the Technology Councils of North America (TECNA), we would be very happy to help connect NIST to these groups. We would suggest engaging state and regional technology councils in roundtable discussions to hear directly from them before further changes are made to the framework.

We would like to again thank NIST for the opportunity to participate in this process. We strongly believe that engaging all segments of the critical infrastructure population on a regular basis is the key for the voluntary framework success. We look forward to continuing to work with you on this and would welcome the opportunity to further engage with you.