CompTIA

The Computing Technology Industry Association
Docket No.: 13090978 – 378 – 01
National Institute of Standards and Technology
Request for Comments on the Preliminary Cybersecurity Framework

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

On behalf of CompTIA, thank you for the opportunity to provide comments on the NIST framework entitled, "Improving Critical Infrastructure Cybersecurity Executive Order 13636." CompTIA has been an active participant in this process, attending three workshops on this matter, and engaging with NIST staff during the last several months. We appreciate the opportunity to be an active partner and look forward to continuing our dialogue.

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 feedback on the draft revolves around two main priorities: 1) the ease with which small and medium sized business (SMBs) can adapt the framework; and 2) the capability to have a trained and certified workforce to carry out the framework functions. SMBs are an integral part of our cybersecurity ecosystem and often enjoy critical partnerships with larger organizations and government. However, their resources, both financial and in manpower, must be a consideration in standard setting, voluntary or otherwise. Additionally, the capability of the workforce, both in the private sector and at the federal level, to operate technology and carry out functions in a way that minimizes cybersecurity threats is critical to the broader objective of achieving a reliable bulwark against cyber threats.

Adoption by Small and Medium Sized Businesses

Depending on the definition used, the number of SMBs that own or operate critical infrastructure ranges from 4,620 to 13,861[1]. Using even the most conservative estimate, this still represents a large number of organizations that may wish to comply with the voluntary framework. As such, this framework must be navigable to organizations of all sizes. Use of a common lexicon when describing security issues is especially critical in order to facilitate wide spread adoption by the SMBs. There is a gap between executives (44%) and IT function employees (70%) when viewing security change, with the latter more inclined to view such efforts as "drastic" and the former underestimating the effort that goes into such work.[2] Attention to language could ease some of these miscommunications and lower the resistance to adoption. The framework is an ideal

[1] U.S. Economic Census, 2010.

[2] CompTIA report, "Information Security Trends," November 2013.

place to help establish this common lexicon.

Another concern as it relates to the SMB community is general awareness and understanding of the framework. While the framework presumes that a company will have certain resources, SMBs often lack an IT staff and a security infrastructure. The typical SMB is focused on day-to-day operations and limited bandwidth gives little ability to entertain state/federal voluntary compliance regimes. As such, incentives for adoption for SMBs are an option that should be explored. The private sector has already begun to link security practices to an industry-recognized organizational credential or other voluntary assessment. This avenue provides complying businesses with a market differentiator and can be used to retain and/or bring in new business. Efforts should be explored to help motivate businesses to divert already scarce resources to framework implementation.

We would also suggest providing an online interactive tool in which SMBs can share experiences in implementing the framework. Simply put, the framework can be overwhelming to SMBs as they are not as familiar with the process and the reasoning for its creation. Nor do they have manpower that can be dedicated to interpreting the various options. This sense of being "overwhelmed" could create a chilling effect and stop organizations from implementing the framework. The Small Business Administration, an entity already known to many of the SMBs, would be an ideal place for this online tool to reside. We would recommend that this online interactive tool enable organizations to post and review best practices, case studies, challenges, and other experiences related to implementation on a live website that can be organized in any variety of ways. This "crowd-sourcing" of implementation can not only create a community feel for the SMBs, but also maximize resources when implementing the framework.

The Cyber Workforce

The issue of cyber workforce is one on which NIST has been actively engaged and CompTIA has enjoyed a productive partnership with NIST on this matter. As it relates to the framework, cyber workforce is crucial, as it will take a trained and certified workforce to implement and continually monitor organizational security. CompTIA works in collaboration with thousands of academic and vendor-specific IT training programs around the world. Through our experience, and in tandem with research, we know that industry certifications in IT raise the effectiveness of an IT team in carrying out its job functions. Moreover, testing and assessment in education settings can, among other things, identify gaps in knowledge, develop retrieval aids that enhance retention of knowledge, and improve transfer of knowledge to new contexts. A recent study revealed that 86 percent of firms believe that certified staff members deliver a high or moderate return on investment when it comes to improving organizational security. Furthermore, 66 percent agree or strongly agree that IT professionals with security certifications are

more valuable to the organization[3].

This understanding and support for industry-recognized certifications is a fundamental tenet of the National Initiative for Cybersecurity Education (NICE). CompTIA has been involved in the NICE initiative, particularly as it relates to professionalization and training of the workforce. This component aims to develop and maintain a globally competitive cybersecurity workforce by way of standards and strategies for cybersecurity training and professional development.

We are helping to establish standards for professionalizing the cyber workforce by working with the Department of Homeland Security (DHS) during the creation and launch of the National Initiative for Cybersecurity and Studies (NICCS) portal. The portal is designed to be an online resource for those who are looking to enter the cybersecurity workforce or to advance their careers by mapping industry recognized certifications to knowledge, skills and abilities (KSAs) required for government careers. This is being done in cooperation with the NICE National Cybersecurity Workforce Framework, which provides a common understanding of and lexicon for cybersecurity work. The Framework is based on "Categories" and "Specialty Areas" which are used to organize similar types of work. Within each specialty area, common tasks and KSAs are provided. The intention of the framework is to standardize the descriptions of cybersecurity work regardless of where and by whom it is being performed. CompTIA provided input on this framework and is now working, through DHS and with our partners in the Cybersecurity Credentials Collaborative (C3), to map industry credentials to the 31 specialty areas identified in the Framework.

This work is important to us as almost every U.S. federal government agency and major contractor employs IT workers who hold one or more CompTIA certifications as a part of their IT workforce development strategies. CompTIA certification vouchers appear on GSA schedules and other government contract vehicles available from CompTIA-authorized partners. CompTIA certification is portable across divisions, sectors, and international boundaries. Yet, while this is all beneficial, the fact remains that there is no organized approach to the training and credentialing of the federal workforce. The NICE initiative recognizes the value of certifications as a symbol of ability, and also as a way to professionalize the cyber workforce.

We were pleased to see a reference to this in the framework on page 41 of the draft, but we believe that there should be a more concrete connection between the NIST cybersecurity framework and the NICE framework. Many private sector organizations that are implementing the framework will need to expand, if not establish, their cybersecurity workforce. These organizations would greatly benefit from the work that is being done in establishing a common lexicon and a clear career path into cybersecurity through the NICE framework. Furthermore, organizations that are just beginning to build an internal workforce or are looking to outside organizations for their cybersecurity

---

[3] CompTIA report, "Information Security Trends," November 2013.

personnel needs, will no doubt require some guidance on what to look for. The NICE framework can help to translate the skills an organization needs to what an individual or an organization may possess. We would be pleased to work with NIST on this expansion.

In conclusion, we believe the framework is an excellent first step in helping to secure our nation's critical infrastructure. In refining the framework, a focus on the needs of SMBs will enable organizations of all sizes to more readily able to adopt the framework. Furthermore, a deeper connection between our cybersecurity and the workforce needed to ensure this security will strengthen the framework's effectiveness. We look forward to continuing to work with NIST and are happy to answer any questions related to any of our above suggestions.

About CompTIA

CompTIA is a non-profit high tech trade association made up of more than 2,000 members and more than 2,000 partners. CompTIA's members are at the forefront of innovation and provide a critical backbone that supports broader commerce and job creation. Our membership includes computer hardware manufacturers, technology distributors, and IT specialists who help organizations integrate and use technology products and services. We are also the leading developer and provider of vendor-neutral IT workforce certifications. CompTIA certifications most commonly recommended or required by federal agencies (CompTIA A+, CompTIA Network+, CompTIA Security+ and CompTIA Advanced Security Practitioner) are International Standard ANSI/**ISO**/IEC 17024 certified. Our partners include worldwide training and testing developers, training providers, and academic institutions.

As an organization, we support policies that expand life-long education in the computer sciences and basic IT skills. We support secure and smart IT solution policies in the area of cybersecurity, data breach, privacy, and cloud computing. We are committed to closing the skills gap that our nation is facing. In short, we believe that millions of Americans can obtain a high wage IT job through the process of training for, and obtaining, an IT workforce certification. Significant business and government efficiencies can be achieved with respect to IT maintenance, data, and security if America's workforce has the appropriate training and credentialing.