Mr. Michael Hogan and Ms. Elaine Newton
Office of the Director, Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive
Mail Stop 8930
Gaithersburg, MD 20899-8930

September 24, 2015

Re: Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (NISTIR 8074 Volume 1 (Draft))

Mr. Hogan and Ms. Newton:

CompTIA thanks the National Institute of Standards and Technology (NIST) for the opportunity to comment on the "Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity" (NIST IR 8704 Volume 1 (Draft)).

As you may know, CompTIA is a non-profit, high tech trade association with a membership of more than 2,000 that includes computer hardware manufacturers, technology distributors, and information technology (IT) specialists who help organizations integrate and use technology products and services. CompTIA's members are at the forefront of innovation and provide a critical backbone that supports broader commerce and job creation. Our partners include worldwide training and testing developers, training providers, and academic institutions.

Our association is also the leading developer and provider of vendor-neutral IT and cybersecurity workforce certifications. The CompTIA certifications that are 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. We have also recently completed our full integration of TechAmerica into our public advocacy efforts, adding an additional member base of large technology companies and complementing CompTIA's strengths in education, certification, advocacy, and philanthropy with additional competencies in state, federal and international policy work.[1]

We applaud NIST for developing a framework for the U.S. Government's strategic objectives for pursuing the development and use of international standards for cybersecurity. Like NIST, CompTIA believes the increasing complexity and global nature of the world economy, as well as advances in technology, necessitates the coordinated development of international standards to ensure the

[1] *CompTIA Unifies Brand for Advocacy Efforts, June 15, 2015, http://www.comptia.org/advocacy/briefing-room/press-releases/2015/06/15/comptia-unifies-brand-for-advocacy-efforts*

cybersecurity and resiliency of all U.S. information and communications systems and supporting infrastructures. We also want to take this opportunity to again thank NIST for its emphasis on engagement with the private sector on the development international cybersecurity standards. While the majority of our sales of certifications are conducted within the U.S., CompTIA has recently seen growing interest in our certifications and our training companion tools abroad. Currently, about thirty percent of our business is conducted overseas.

Our response to the draft report is centered on NIST's omission of cyber workforce issues as a core area of cybersecurity standardization. As the report rightly points out, "The U.S. standardization community is comprised largely of non-governmental Standards Developing Organizations (SDOs)." This observation is very prevalent in the IT cyber workforce space and industry solutions to achieve a skilled workforce align with the U.S. Government focus on achieving cost-efficient, timely, and effective solutions for mission and policy objectives. CompTIA has also provided some additional feedback on effective U.S. Government programs that we encourage NIST to consider as it strives to achieve standardization across the global cyber workforce.

First, the capabilities of the global cyber workforce both in the private sector and within government must be a consideration in standard setting. CompTIA urges the Executive Office of the President (EOP) interagency policymaking body and the Department of Commerce's International Cybersecurity Standardization Working Group, as envisioned by the draft report, to consider cyber workforce issues as a core area of cybersecurity standardization. ***We believe the best way to protect U.S. information in today's global environment is to ensure that all IT and cybersecurity professionals with access to sensitive information receive not only the appropriate training to carry out their job responsibilities, but also achieve industry-recognized certifications that designate and validate the appropriate skills sets. To clarify, CompTIA is not seeking the development of an international standard that dictates uniform training programs and specific certifications, but rather is seeking the codification of an approach that includes certification in addition to training as a best practice.*** As most cyber incidents are the result of human error, CompTIA believes the standardization of providing cybersecurity training and certification programs may be the most significant step the U.S. Government and its foreign partners can take to protect U.S. data in the global information environment.

Further, should the U.S. Government pursue cyber workforce training and certification issues as a core area of cybersecurity standardization, we believe there are lessons to be learned from the Department of Defense's (DOD) implementation of IT and cybersecurity training and certification programs, as well as the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework in the development of best practices pertaining to the cyber workforce. CompTIA urges NIST to consider these programs as it strives for consensus with foreign partners on international cybersecurity standards.

Cybersecurity Training and Certification Can Help Mitigate Vulnerabilities Caused by Human Error

According to research performed by CompTIA, the growing proliferation and sophistication of hackers, combined with greater reliance on interconnected applications, devices, and systems, has created a security environment that is challenging for even the best-prepared organizations. Against this backdrop, it is not surprising that CompTIA's April 2015 "Trends in Information Security" report found that the biggest weak spots that lead to cybersecurity breaches are human users of IT.[2]

Though human error often ranks low as a serious concern for organizations, CompTIA's research has shown it is the largest factor behind security breaches. Most recently, human error has been proven to be the cause of 52 percent of all cybersecurity breaches in the workplace.[3] This should not be surprising as large organizations, such as federal government agencies, often make use of thousands of computers in order to carry out their daily missions. When a human being is put in front of those computers, they each bring a level of cybersecurity risk. This necessitates the need for a well-trained IT and cybersecurity workforce with the proven capabilities to identify, mitigate, and respond to risk. With regard to human error, training is the clear answer, but many public and private organizations today struggle with understanding how to afford, access, and institutionalize meaningful investments in training and other solutions, such as certifications, that can better prepare staff tasked with cyber hygiene to operate in today's environment.

As noted above, IT security is increasingly essential to successful government operations. Maintaining and increasing IT organizational performance in key areas such as IT support and IT security are import goals for all Chief Information Officers (CIOs) and IT leaders. Studies have shown that industry-recognized certifications in IT raise the effectiveness of an IT team in carrying out its job functions. Moreover, according to third party studies on testing versus training, testing in educational settings can, among other things, identify gaps in knowledge, develop retrieval aid that enhance retention of knowledge, and improve the transfer of knowledge to new contexts.

We have also conducted research on managers' perceptions of the importance of testing after training, specifically at DOD. CompTIA's Military Career Path Study found that 74 percent of active duty military personnel with staff management responsibilities classified testing after training to confirm knowledge gains as "very important."[4] Further, these managers reported that testing after training also helped to set a baseline of expertise among staff, provide career path guidance, improve the performance of a team, retain talented staff, and evaluate staff for promotions or career advancement.[5]

According to a study conducted by the International Data Corporation (IDC) and sponsored by CompTIA, candidates and staff with CompTIA A+ and CompTIA Security+ certifications perform better than staff that is not certified. This research found that certified employees are: (1) more confident; (2) more knowledgeable; (3) reach job proficiency more quickly; (4) more reliable; and (4) perform at a higher level.[6]

[2] CompTIA. *Trends in Information Security Study*. CompTIA; 2015. Available at: http://www.comptia.org/resources/trends-in-information-security-study?c=24290.

[3] *Id.*

[4] CompTIA. *Military Career Path Study: Assessing the Role of Training and Certifications.* CompTIA; 2014. Available at: http://www.slideshare.net/comptia/military-it-career-path-study.

[5] *Id.*

[6] CompTIA. *IT Support and Security Performance: The Impact of CompTIA Certifications on Organizational Performance*. International Data Corporation (IDC); 2014. Available at: https://certification.comptia.org/docs/default-source/audience-pdfs/comptia-ebrochure_impact-of-certification-on-performance.pdf?sfvrsn=2.

When IT professional are confident in their abilities, they are more likely to be forward thinking, proactively anticipate issues, and solve problems before they impact organizational performance. Having the right skills gives IT professionals the confidence to believe they can achieve their assigned responsibilities. Further, certified professionals are 85 percent more likely to believe they have the knowledge and skills needed to successfully fulfill their jobs.[7] As a result, these certified security professionals are better positioned to properly assess risks, design and implement interventions, and correct policy weaknesses. Because most of today's hiring environments prioritize experience above professional credentials, it is also important to note that CompTIA's research has found that after ten years of security experience or support experience, certified staff has between 20 and 25 percent more core domain knowledge than those with the same experience who are not certified. Once on the job, certified IT professionals have also been found to perform up to 53 percent better than those without certification in critical, job-related activities.[8]

Further, certifications help to put program managers at greater ease with the capabilities of their staff. Research conducted by CompTIA has found that an overwhelming majority of IT professionals and their hiring managers agree on the value of certifications. Ninety-three percent of human resources (HR) executives believe certifications are beneficial, as they offer a competitive edge in the job market, heightened career advancement opportunities, and increased value to employers and their organizations.[9] According to employers, the top benefits of IT certification are: (1) the ability to understand new or complex technologies; (2) higher productivity; and (3) more insightful problem, solving.[10] In addition, CompTIA has found that roughly eight in ten hiring managers say it is challenging to find the right candidates with the right skill sets to fill vacant IT positions and verifying job candidates' credentials can be a challenge.[11]

Lessons Can Be Drawn From the Implementation of Department of Defense Directive 8570 and the Issuance of Department of Defense Directive 8140

As many U.S. federal government agencies and foreign government agencies do not already have robust IT and cybersecurity training and certification programs in place, CompTIA believes NIST may be able to draw upon lessons learned by both the public and private sectors through the implementation of DOD Directive (DODD) 8570 and the issuance of DODD 8140, DOD's newest directive on cyber workforce management.

By way of background, DODD 8570 and the corresponding instruction manual (DODD 8570.01-M) guarantee that every full- and part-time military service member, defense contractor, civilian, and foreign employee with information assurance (IA) responsibilities and privileged access to DOD

[7] *Id.*
[8] *Id.*
[9] Carrado A. Four Reasons HR Execs Love Certifications. *CompTIA IT Careers Blog*. 2015. Available at: http://certification.comptia.org/news/2015/05/29/four-reasons-hr-execs-love-certifications.
[10] *Id.*
[11] *Id.*

systems obtains IT certification.[12] This program enhances U.S. national security, ensures value from taxpayer investments in IT training, and helps our veterans transition their skills to civilian employment once their military service has ended. CompTIA is proud to be a partner to DOD in its implementation of this directive.

Prior to the issuance of DODD 8570 in 2004/2005, DOD relied on longstanding guidance and memorandum for the training of its cyber workforce. While these guidance and memorandum were useful, interim guidelines left individual components to decide what to do to comply. This resulted in wide variation in implementation across the Department and a situation where the certificate of one component was not recognized by other components, triggering the need for standardization under DODD 8570. It took two years to draft DODD 8570 and another year to issue the manual, which specified baseline certifications, including those provided by CompTIA.

This DOD program has been so successful that both the House[13] and the Senate[14] included language in their respective FY16 National Defense Authorization Acts (NDAAs) directing DOD to expand its certifications program to include all DOD personnel identified as critical to network defense, as opposed to just those with IA job titles. Given the amount of federal money invested on training, CompTIA believes that DOD's marginal investment in these additional certifications will go a long way in strengthening DOD's cybersecurity posture. As a result, CompTIA would like to see other U.S. Government civilian agencies, as well as foreign government agencies, adopt similar, standardized programs for not only training, but also for certifying their cyber personnel.

While Congress has directed DOD to expand its IT and cybersecurity training and certification programs, DOD is already undertaking its own efforts to expand these programs to improve the security of DOD networks. This August, DOD issued DODD 8140, its new high-level directive on cyberspace workforce management.[15] DOD will now begin the process of drafting the instruction manual for carrying out the new the policy, which is likely to expand the emphasis on industry-recognized certifications. At a minimum, this process will span the next year, and could possibly stretch into the next three years. While DODD 8140 will replace DODD 8570, DOD will continue to use the DODD 8570 manual as a stand-in for the 8140 manual under development.[16] CompTIA believes the issuance of DODD 8140 demonstrates the priority DOD places on its IT and cybersecurity training programs and would like to see other government agencies make a similar commitment.

The Importance of Professional Certifications as Outlined by the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework

[12] U.S. Department of Defense. *DODD 8570.1-M: Information Assurance Workforce Improvement Program (Incorporating Change 3, January 24, 2012)*. Defense Technical Information Center; 2012.
[13] National Defense Authorization Act for Fiscal Year 2016, H.R. 1735, 114th Cong. §570a (2015).
[14] U.S. Senate, Committee on Armed Services. *National Defense Authorization Act for Fiscal Year 2016 Report,* S. REP. NO 114-49 (2015).
[15] U.S. Department of Defense. *DODD 8140.01: Cyberspace Workforce Management*. Defense Technical Information Center; 2015.
[16] Stanger J. What are U.S. DODD 8140, 8570 and 8570.01-M and What Do They Mean for Your Career?. *CompTIA IT Careers Blog*. 2015. Available at: http://certification.comptia.org/news/2015/09/11/what-are-u.s.-dod-8140-8570-and-8570.01-m-and-what-do-they-mean-for-your-career-.

While the draft report does not explicitly recognize cyber workforce issues as a core area of cybersecurity standardization, CompTIA was pleased to see NIST articulate the need for the U.S. Government to support standardizing education in technical and graduate educational programs, especially in engineering, business, sciences, and technology, to ensure the development of future generations of cybersecurity standards participants. We were also pleased to see NIST explicitly encourage building upon NICE. The issue of promoting a qualified cyber workforce is one on which NIST has been actively engaged and CompTIA has enjoyed a productive partnership with NIST on this matter.

CompTIA notes that understanding and support for industry-recognized certifications is a fundamental tenet of NICE's National Cybersecurity Workforce Framework.[17] CompTIA has been involved in the NICE initiative, particularly as it relates to professionalization and training of the workforce. This component of the NICE strategy aims to develop and maintain a globally competitive cybersecurity workforce by way of standards and strategies for cybersecurity training and professional development.

As background, CompTIA was an active participant in 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, which is now active, was designed to serve as an online resource for those 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 was done in cooperation with the NICE National Cybersecurity Workforce Framework, which, as previously mentioned, 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 was to standardize the descriptions of cybersecurity work regardless of where and by whom it is being performed. CompTIA provided input on this Framework and has worked through DHS and with our partners in the Cybersecurity Credentials Collaborative (C3)[18], to map industry-recognized credentials to the 31 specialty areas identified in the Framework. CompTIA has also been engaged in more recent conversations with NIST regarding how this work may be expanded and we look forward to continuing this partnership.

The mapping of industry-recognized certifications to specific career paths is especially important to CompTIA, as many U.S. federal government agencies and major contractors employ IT workers who hold one or more CompTIA certifications as part of their IT workforce development strategies. While this is the case for the U.S. Government, it is also important to note that CompTIA certifications are portable not only across divisions, agencies, and business sectors, but they are also transferable across international boundaries. While this is beneficial to the cyber workforce that is becoming more global in nature, the fact remains that there is no organized approach to the training and credentialing of either the U.S. government or foreign government cyber workforces.

[17] National Initiative for Cybersecurity Education. *The National Cybersecurity Workforce Framework*. National Institute of Standards and Technology; 2014.

[18] http://www.cybersecuritycc.org/

The NICE initiative recognizes the value of certifications as a validator of ability, and also as a way to professionalize the cyber workforce. For this reason, CompTIA agrees NICE should be given extensive consideration as the foundation for an international standard on credentialing the cyber workforce. CompTIA also acknowledges that overseas partners may only be in the initial stages of building an internal cyber workforce or may have reached a point where their cyber staff may need to expand. These organizations would greatly benefit from whatever guidance the U.S. Government can provide based on its experience with the NICE Framework.

Conclusion

In conclusion, CompTIA thanks NIST for outlining a thoughtful approach to strategic U.S. Government engagement in pursuit of the development of international cybersecurity standards. In refining this approach, CompTIA urges NIST to elevate cyber workforce issues as a core area of cybersecurity standardization. By ensuring a qualified cyber workforce, the U.S. Government and its international partners can meet target objectives for other core areas of cybersecurity standardization, including cryptographic techniques, cyber incident management, identity management, IT system security evaluation, information security management systems, network security, security automation and continuous monitoring, supply chain risk management, software assurance, and system security engineering.

To reiterate, CompTIA believes training *and* certification are valuable components of any cyber workforce management strategy. We are not advocating for an international requirement in support of uniform training and specific certifications. Instead, CompTIA is looking to NIST to support an international standard that embraces certification wherever investments are made in IT training. We have found there are strong examples of robust training and certification programs within the U.S. Government and we encourage NIST to highlight these examples in its ongoing dialogue with U.S. Government agencies and their foreign counterparts in the development of international cybersecurity standards. We look forward to continuing our work with NIST and would be happy to answer any questions related to the feedback above.

Respectfully submitted,

Elizabeth Hyman
Executive Vice President, Public Advocacy
CompTIA