Kevin Kimball
Chief of Staff
National Institute of Standards and Technology
100 Bureau Drive, Stop 200
Gaithersburg, MD 20899

RE: Cybersecurity Workforce RFI [Docket Number 170627596-7596-01]

BSA | The Software Alliance (BSA)[1] is grateful for the opportunity to provide comments to the National Institute of Standards and Technology (NIST) on strengthening the cybersecurity of federal networks and critical infrastructure through workforce development.

BSA is the leading trade association representing the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, developing cutting-edge solutions in use across the range of information technology (IT) platforms, and are global leaders in advancing cybersecurity.

BSA is grateful to NIST and the National Initiative for Cybersecurity Education (NICE) for bringing focus on developing the cybersecurity workforce. As BSA's members are keenly aware, workforce development remains one of the most significant challenges to effective cybersecurity, in both the public and private sector. As NICE has documented, over 1.5 million global cybersecurity jobs are expected to be unfilled by 2020, leaving government and industry stakeholders at risk of substantial vulnerabilities in our defenses against cyberattacks.[2] ISACA's recent report, *State of Cyber Security 2017: Current Trends in Workforce Development*, finds that among surveyed companies approximately a quarter of all cybersecurity positions remain unfilled; compounding this challenge, even those jobs that can be filled often take months to fill and receive few applications from qualified

[1] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Docusign, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro, and Workday.

[2] NIST factsheet "Cybersecurity Workforce Demand." https://www.nist.gov/sites/default/files/documents/2017/01/30/nice_workforce_demand.pdf.

candidates.[3] As a recent study conducted jointly by the Center for Strategic and International Studies and Intel Security found, "This shortage in cybersecurity skills does direct and measurable damage."[4]

I. Industry leadership is making a difference.

Because of the importance of effective cybersecurity to innovation and digital commerce, BSA's members are highly invested in training, developing, and retaining a cybersecurity workforce that is sufficiently skilled, diverse, and robust enough to meet the rapidly growing demand. For that reason, its members invest heavily in workforce development at several points along the trajectory of an individual's education and professional training. Nearly all BSA members invest directly in programs working to provide education, training, and other resources to current and future cybersecurity professionals. These programs include education initiatives to engage youth in the K-12 education system in computer science education and other Science, Technology, Engineering, and Mathematics (STEM) disciplines; support programs at community colleges, vocational institutions, polytechnic schools and career centers; develop new educational models to connect classroom learning with potential career directions; recruit and fund scholarships for talented youth to enroll in university computer science and related programs; donate technology-based educational platforms to university STEM programs; sponsor cybersecurity competitions; and create broad-based digital literacy curricula. BSA's members also invest in training initiatives to support on-the-job training through apprenticeship and internship opportunities; specialized mid-career training for veterans and their spouses; targeted apprenticeship programs for urban youth; expanded adult education opportunities; and comprehensive continuing education and training programs for current employees. In addition, BSA members have developed innovative approaches to diversify the cybersecurity workforce, such as targeted outreach and recruiting initiatives focusing on underrepresented populations; organizing professional organizations in support of female and minority cybersecurity professionals

These efforts are making a real and important difference, leading to the incorporation of thousands of new professionals into the cybersecurity workforce. However, given the rate of growth of cybersecurity jobs, industry efforts alone will not be sufficient to bridge the gap. Building on efforts already underway through NICE and other initiatives, BSA believes addressing the cybersecurity workforce shortfall will require expanded collaboration between government and private industry to improve cybersecurity education, expand alternative pathways to cybersecurity careers, and expand opportunities for re-training of mid-career professionals.

---

[3] ISACA, *State of Cyber Security 2017: Current Trends in Workforce Development.* http://www.isaca.org/Knowledge-Center/Research/Documents/state-of-cybersecurity-2017_res_eng_0217.pdf?regnum=384605.

[4] Center for Strategic and International Studies and Intel Security, "Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills." https://csis-prod.s3.amazonaws.com/s3fs-public/160727_rpt_cybersecurity_workforce_shortage.pdf.

II. Improving cybersecurity education.

Building a cybersecurity workforce to meet current and future needs begins with educating a broader generation of future practitioners. NICE and other initiatives made important contributions to enhancing education opportunities to support development of the cybersecurity workforce. The establishment of cybersecurity academic centers of excellence and the Community College Cyber Summit, support through scholarship programs such as *Cybercorps: Scholarship for Service* and the *Department of Defense Cybersecurity Scholarship*, the Department of Homeland Security's efforts to develop a K-12 cyber-based curriculum, and innovative efforts to engage youth such as *GenCyber* have all proven successful, albeit on a relatively small scale. And the creation of the NICE Cybersecurity Workforce Framework has provided an important baseline to shape an understanding of what skills and capabilities are important in developing cybersecurity professionals, both in the classroom and through specialized training.

To address the scope of the cybersecurity workforce gap, these efforts must be expanded. Funding for existing cybersecurity education efforts, including the *CyberCorps: Scholarship for Service* and *Department of Defense Cybersecurity Scholarship* programs, should be increased to reflect the urgency of the need. In addition, the government should invest in new programs to address to critical challenges: first, to incentivize the development, accreditation, and promotion of more cybersecurity-focused education programs through community colleges and other educational venues that do not provide 4-year degrees, which can be cost-prohibitive and are often unnecessary for cybersecurity positions; and, second, to incentivize more female and minority students to pursue cybersecurity education, to address tremendous imbalances in the current workforce. Such efforts should be reinforced through deepening interagency coordination of existing policy initiatives and funding and levers to enhance cybersecurity education and training.

Women and minorities represent only 11% and 12% of cybersecurity professionals, respectively – statistics that indicate a dangerous inability to leverage the talents and perspectives of huge segments of the American workforce.[5] As with wider efforts to provide education to cybersecurity professionals, BSA member companies invest in a range of programs aimed at increasing representation of women and minorities in the technology industry workforce. BSA itself, for example, through its nonprofit foundation Software.org partners with Girls Who Code to sponsor the Summer Immersion Program, giving a class of young women the chance to learn coding skills and gain exposure to technology careers. These efforts will help the industry engage with underrepresented portions of the population – and reap the economic and innovative benefits of a more diversity workforce.[6] As with training efforts, however, properly increasing the diversity of the workforce will require

---

[5] Simone Petrella, "Cybersecurity's Dangerous Game of Chicken," New America Foundation. https://context.newamerica.org/cybersecuritys-disastrous-game-of-chicken-151657baf41e.

[6] K. W. Phillips, "How diversity makes us smarter," Scientific American https://www.scientificamerican.com/article/how-diversity-makes-us-smarter/.

expanded collaboration between government and private industry through efforts to expand proven training strategies.

III. Expanding alternative pathways to cybersecurity careers.

The cybersecurity workforce need not be a monolithic cast of students with 4-year degrees in computer science; in fact, studies have suggested that computer science degree programs do not necessarily prepare students effectively for cybersecurity careers.[7] Cybersecurity expertise can be developed through alternative pathways that do not require four-year college or graduate degrees, including through apprenticeship programs, community colleges, cybersecurity "boot camps" or short-term intensive training academies, and relevant government or military service. The federal should invest in fostering these alternative pathways.

Priority should be placed on capturing the talent developed through the United States Military. As the military becomes more technologically sophisticated and engaged in cybersecurity activities, it has become a dynamic breeding ground of talented information technology and cybersecurity professionals; however, these military personnel may have challenges in translating military-specific skills into civilian government or private sector positions. The Air Force's VetSuccess program, which provides specialized cybersecurity training to personnel transitioning into non-military careers, has demonstrated promise and should be expanded across the military services. Expanding cyber-centric opportunities available to transitioning servicemembers and veterans through SkillBridge, GI Bill benefits and vocational rehabilitation programs would also help capitalize on the military's vast reservoir of talent.

Similarly, quality apprenticeship programs and educational models that connect classroom education to professional skills development offer great promise in generating talented, trained cybersecurity professionals. BSA's members have invested significant resources in such programs; government investment in these efforts could expand their scope and effectiveness considerably. To this end, BSA and its members are eager to work with the *ApprenticeshipUSA* initiative to ensure federal support for apprenticeships is leveraged to enhance the cybersecurity workforce.

IV. Expanding re-training opportunities for mid-career professionals.

While investing in educating young people to fill the cybersecurity jobs of tomorrow is critical, the growth of digital commerce is proceeding at a pace that requires an influx of new cybersecurity professionals now; we cannot expect new generations of professionals to fill the gap alone. Investing in expanding re-training opportunities to enable mid-career professionals to transition into cybersecurity careers could help bridge the cybersecurity workforce shortfall in the near-term, while also helping the American workforce evolve to support the changing demands of the 21st-Century economy.

---

[7] Center for Strategic and International Studies and Intel Security, "Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills." https://csis-prod.s3.amazonaws.com/s3fs-public/160727_rpt_cybersecurity_workforce_shortage.pdf.

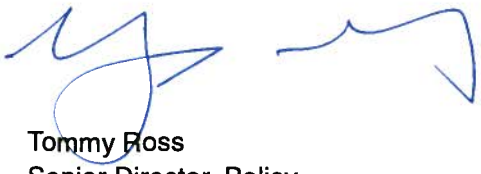
While digital commerce has brought millions of jobs to the American economy, it has also left some workers behind, as technology has reshaped industries ranging from manufacturing to food services. New investments in re-training, as well as redirecting current re-training programs, can help these workers find new opportunities in the digital economy. Efforts to re-train Americans losing traditional jobs due to trade and digitalization should be expanded, and should focus on providing these individuals with high-demand skills in cybersecurity and information technology. The Trade Adjustment Assistance (TAA) program should be reexamined as a potential tool for such re-training. TAA was established to provide mid-career retraining to employees who jobs are impacted by globalized trade; the digital economy can pose similar challenges, but the growing availability of jobs in the new digital economy can also be part of the solution. TAA could be modified and expanded to serve individuals who jobs are impacted by digitalization, and to provide dedicated program support to cybersecurity and information technology-focused training.

V. Conclusion

Meeting the demands of the cybersecurity workforce is an imperative for both our economy and national security. Achieving this goal requires a dynamic partnership between the U.S. government and private industry, and robust investment in creating new and innovative approaches to educating and training cybersecurity professionals. BSA and its members have been leaders in fostering such approaches, and are eager to work with NIST and other stakeholders to build upon recent successes. Bridging the workforce development gap will not happen overnight, but will require sustained investment on behalf of both government and industry to confront the challenge.

Thank you for the opportunity to comment on this important matter.

Sincerely,



Tommy Ross
Senior Director, Policy

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org