On "Growing and Diversifying the Cyber Talent Pipeline"

A Hearing Before the

House Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection and Innovation

Written Testimony Submitted by Laura Bate
Policy Analyst, New America

May 21, 2019

--

Chairman Richmond, Ranking Member Katko, Members of the Subcommittee, thank you for the opportunity to provide written testimony for today's hearing on "Growing and Diversifying the Cyber Talent Pipeline." The members of this Subcommittee undoubtedly understand the critical importance of effective cybersecurity. Protecting data and information systems throughout the federal government and military is fundamental to protecting national security, but our considerations must extend beyond that.

The nation's economic health is a building block of national security. The United States is currently losing between $57 and $109 billion dollars a year to cybersecurity failures.[1] Fostering an environment in which major corporations, small and medium enterprise, and individuals can curtail these losses and secure their own digital assets is integral to providing homeland security. This undertaking is only possible if the United States can cultivate a strong, skilled cybersecurity workforce, not just within the federal government, but throughout the whole of the economy.

I work with partners in higher education, private industry, and public service to improve our understanding of the dynamics that shape the cybersecurity workforce. As a policy analyst with the Cybersecurity Initiative at the think tank New America, my research encompasses both how

[1] Council of Economic Advisors. *The Costs of Malicious Cybersecurity Activity to the US Economy*. Executive Office of the President of the United States, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. (Accessed May 2019).

we expand that workforce and how we strengthen it through diverse perspectives and educational pathways that evolve to meet the challenges of cybersecurity's changing landscape.

I have been encouraged to see both Congress and the Administration redouble efforts to fill cybersecurity jobs in recent weeks. The introduction of new proposed legislation from both Chambers of Congress and on both sides of the aisle is an important step, as is the President's Executive Order on America's Cybersecurity Workforce. As commendable as these steps are, however, they are only a part of a very long path to filling the empty chairs in the U.S. cybersecurity community. I will focus on three particular aspects of this challenge: 1) the critical need for building a more diverse workforce, 2) incentivizing the development of apprenticeships and other new pathways into cybersecurity jobs, and 3) improving our understanding of the workforce through empirics.

Diversity Is a Feature of Strong Cybersecurity Teams

Diversity is critically important in the cybersecurity workforce for three reasons:

1. Inadvertently limiting diversity artificially narrows hiring pipelines. We cannot afford to overlook entire demographics when we consider the pool of available talent. The United States needs to fill more than 300,000 cybersecurity jobs. There are an estimated 715,715 workers currently employed in cybersecurity jobs,[2] which means that the industry must grow by more than forty percent just to meet current needs, let alone future requirements. Given the scale of the demand and the importance of these jobs, the country is best served by prioritizing the identification and removal of the barriers that discourage diversity in the cybersecurity industry.

2. Diversity makes teams stronger. Research indicates that diverse teams focus more on facts, process those facts more carefully, and are more innovative.[3] Because we are discussing the teams that will protect Americans' lives and livelihoods, we cannot afford to field anything less than the best teams possible.

3. Cybersecurity jobs pay well. Ensuring that these economic opportunities are equally accessible to all members of our communities is simply the right thing to do.

[2] *Cybersecurity Supply/Demand Heat Map*. CyberSeek. https://www.cyberseek.org/heatmap.html. (Accessed May 2019).
[3] Rock, David and Heidi Grant. *Why Diverse Teams are Smarter*. Harvard Business Review, November 4, 2016. https://hbr.org/2016/11/why-diverse-teams-are-smarter. (Accessed May 2019).

Increasing diversity, equity, and inclusion within the workforce is not an easy task. Successful efforts require more than a policy or law; they require significant structural and cultural changes throughout the entire education and training ecosystem. Such widespread change takes time and deliberate effort. To support this goal, policymakers must make workforce diversity an integral and explicit feature of future cybersecurity workforce development programs.

When diversity is not an explicit consideration in the creation of new programs, innovations that might otherwise be beneficial run the risk of unintentionally decreasing diversity. For example, consider Section 2 (c) of the recent Executive Order on America's Cybersecurity Workforce, which directs Administration leadership to identify and implement aptitude assessments that can be deployed across the non-cybersecurity federal workforce to identify employees who are promising candidates for cybersecurity training.

It is unclear how aptitude would be defined in these tests, but an easy mistake would be to seek out individuals that display characteristics that reflect those of individuals that currently succeed in cybersecurity roles. Such a test could quite possibly identify candidates with backgrounds and experiences similar to the current workforce, thus reinforcing the industry's current demographics. These tests could be very beneficial in rapidly expanding the federal cybersecurity workforce, but if they are not implemented with very careful attention to the impact on diversity, they could do more harm than good.

It is not enough to expect diversity to grow as a byproduct of workforce development programs. Diversity must be an explicit and integral feature of the future cybersecurity workforce.

Innovation Responds to Incentives

Growth in the cybersecurity workforce is hampered by limited opportunities for potential employees to enter the field and gain experience. The most commonly requested professional certification,[4] the CISSP, is not granted in full until candidates can demonstrate five years of relevant work experience.[5] Notably, in the United States there are currently more job postings seeking candidates with this certification than there are certification holders throughout the whole of the economy.[6] The large majority of open cybersecurity jobs require several years' experience in the field and a minimum of a bachelor's degree.[7] [8] The cumulative effect of these requirements

[4] *Cybersecurity Supply/Demand Heat Map*. CyberSeek.
[5] *CISSP - The World's Premier Cybersecurity Certification*. (ISC)². https://www.isc2.org/Certifications/CISSP. (Accessed May 2019).
[6] *Cybersecurity Supply/Demand Heat Map*. CyberSeek.
[7] *Job Market Intelligence: Cybersecurity Jobs, 2015*. Burning Glass, 2015. https://www.burning-glass.com/research-project/cybersecurity/. (Accessed May 2019).
[8] *Cybersecurity Supply/Demand Heat Map*. CyberSeek.

for degrees, certifications, and experience is that it can be quite difficult to find that first job in cybersecurity, especially for job seekers without a degree in computer science or a related field.

Extrapolating from the data available, an estimated 88,000 students graduate from computer and information science programs in the United States in an academic year,[9] and presumably only a small portion of these graduates will choose to go into careers in cybersecurity. Other disciplines like engineering and mathematics also contribute future cybersecurity employees, but nonetheless, it quickly becomes clear that we cannot fill the hundreds of thousands of open jobs with the tens of thousands of available candidates graduating each year.

Filling cybersecurity jobs at scale means that the cybersecurity community must build new ways to bring in employees and build experience. Some large employers and a very few small businesses have developed innovative solutions to provide "on-ramps" for inexperienced employees, but enabling such programs to propagate throughout the economy will require incentives.

Apprenticeship programs offer a particularly promising opportunity to create entry points into cybersecurity jobs. These work-based learning programs provide a way of connecting with more candidates—and particularly those candidates that might otherwise be overlooked by hiring programs that rely on conventional degrees as a filter. Moreover, they provide a means of responding to employers who consistently indicate that they are not finding the skills they need among job applicants.[10] By actually teaching skills in the workplace, employers are integral to shaping their future workforce.

With careful implementation, workers, employers, and educators all stand to benefit from more widespread adoption of cybersecurity apprenticeships.[11] Simply spreading the model, however, is not enough; quality matters in apprenticeship programs. In order for the cybersecurity community to benefit from apprenticeship programs in a sustainable way, measures to expand apprenticeships should support programs that ensure four basic features, drawn from the Apprenticeship Forward Collaborative:

---

[9] The latest official data available is from 2015-2016, in which 64,405 students graduated. Extrapolating from percentage change between years between 2010-2011 to 2015-2016 (49.5%, or 8.25% per year on average), we might expect some 88,436 students to graduate from computer and information science programs during academic year 2018-2019. See: *Table 325.35. Degrees in computer and information sciences conferred by postsecondary institutions, by level of degree and sex of student: 1970-71 through 2015-16*. The National Center for Education Statistics, November 2017, https://nces.ed.gov/programs/digest/d17/tables/dt17_325.35.asp?current=yes.

[10] *State of Cybersecurity 2019: Current Trends in Workforce Development*. ISACA, 2019. http://www.isaca.org/cyber/Documents/state-ofcybersecurity_res_eng_0316.pdf. (Accessed May 2019).

[11] Prebil, Michael. *Teach Cybersecurity with Apprenticeship Instead.* New America, April 14, 2017. https://www.newamerica.org/education-policy/edcentral/teach-cyber-apprenticeship-instead/. (Accessed May 2019).

> "Paid, structured, productive on-the-job training combined with related classroom instruction; clearly defined wage structure with increases commensurate with skill gains or credential attainment; high quality third-party evaluation of program content, apprenticeship structure, mentorship components, and standards to meet business demand and worker need; and ongoing assessment of skills development culminating in an industry-recognized credential and full-time employment."[12]

These characteristics are particularly important in evaluating opportunities to invest in the development of the cybersecurity workforce. Not every program that calls itself an apprenticeship leads to the same benefits. Programs that do not ensure a high level of quality can lead to negative outcomes for the students and the larger cybersecurity ecosystem. Moreover, such programs would divert resources, interest, and credibility from programs that do deliver high-quality learning opportunities.

Responsible support for apprenticeship programs in cybersecurity must also account for local industry requirements. As discussed in New America's prior work, cybersecurity jobs are extremely heterogeneous,[13] and not all cybersecurity work roles are equally in demand in all regions. In order to make best use of resources, policies and legislation to support the expansion of cybersecurity apprenticeships should require rigorous analysis of local job markets to ensure alignment between learners and the specific cybersecurity work roles that are in demand.

Incentives to spark the development of alternative pathways into cybersecurity can take many forms. Such incentive programs could focus on supporting students, for example, through tuition waivers for those pursuing a designated cybersecurity training path.[14] Alternatively, funding could come through competitive grants focused on program development or through reimbursement systems. Tax credits to businesses that utilize emerging systems like cybersecurity apprenticeships, akin to the tax credits proposed in the LEAP Act, could also spur the development of new programs.

---

[12] *Definition and Principles for Expanding Quality Apprenticeship in the U.S.* Apprenticeship Forward Collaborative. https://www.nationalskillscoalition.org/resources/publications/file/Definition-and-Principles-for-Expanding-Quality-Apprenticeship-in-the-U.S..pdf. (Accessed May 2019.)

[13] Bate, Laura. *Cybersecurity Workforce Development: A Primer*. New America, November 1, 2018. https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/. (Accessed May 2019).

[14] There is precedent for such tuition waivers and other systems to support the instructional costs of apprenticeship at the state level, such as in Texas, California, and North Carolina. See https://evolllution.com/revenue-streams/workforce_development/got-you-covered-how-states-can-support-the-costs-of-apprentice-instruction/.

Not all incentives need to come in the way of direct funding. Government can lead by example by implementing innovative models in their own workplaces. Similarly, setting contracting requirements for information technology and cybersecurity services that encourage the promotion of new systems can also be a powerful incentive for the private sector. This is especially true in cybersecurity, where the federal government comprises a particularly large part of the market.

There are many emerging options for increasing the pathways into cybersecurity jobs. Providing incentives to implement these programs widely and continue efforts to innovate further will be key to maximizing the benefit of such programs.

Good Data is Scarce

As different pathways into cybersecurity begin to emerge, establishing mechanisms to evaluate these options will become an important means for allocating resources and improving systems. Right now, the cybersecurity community has very little data on which to base its understanding of the current workforce. A few resources—most notably CyberSeek, a joint project between the National Initiative for Cybersecurity Education, Burning Glass, and CompTIA—provide an understanding of the needs outlined in cybersecurity job postings. However, data on the current workforce is extremely limited.

For example, it is difficult to know which pathways brought current cybersecurity workers to their present positions. Anecdotal evidence would suggest the military, intelligence community, self-taught instruction, and conventional four-year degrees are all major contributors, but we have very little means to judge those in relation to one another or to identify other major pathways. Similarly, we have very little longitudinal data from employees in cybersecurity fields to identify which pathways lead to best outcomes for learners over the course of their career.

Requiring that properly anonymized data collection mechanisms be made a part of government-supported efforts would provide an opportunity to mitigate the current lack of data and would provide a basis on which to evaluate and constantly refine new programs and pathways in cybersecurity education and training. Funding for programs designed to incentivize the development of innovative workforce solutions should include specific requirements for the ongoing analysis of program effectiveness and learner outcomes in order to enable future evidence-based policymaking.

Cybersecurity workforce development is receiving an unprecedented amount of attention from the highest levels of government and industry, and yet we still cannot authoritatively and consistently answer even very basic questions about the current workforce: what percent of the U.S. cybersecurity workforce is female? How many cybersecurity professionals does the U.S.

government employ? What makes a cybersecurity employee—in any role—effective? When these questions are answered at all, the answers vary significantly depending on whom you ask, and the field is rife with studies with inconsistent methodologies and unacceptably small and biased samples.

The lack of credible foundational research in cybersecurity workforce development becomes particularly pernicious when we look towards the future. Current research and rhetoric tends to extrapolate future workforce demand based largely on the growth from the prior year. While it may be intuitive, this approach is overly simplistic and fails to take into account major trends that will shape the future of the cybersecurity industry. Most notably, the increasing reliance on machine learning tools is likely to reduce workforce requirements in some roles while increasing demand for experts in artificial intelligence, roles that often require postgraduate degrees. In order to responsibly invest in the future of the cybersecurity workforce, we must also invest in understanding what that future looks like.

Grants and funding opportunities to develop specific models and types of programs for cybersecurity workforce education and training already exist within the Department of Homeland Security, the National Science Foundation, and other agencies. While these opportunities are critically important to driving innovation, they do not necessarily further our fundamental understanding of the workforce. Providing these agencies with an opportunity to fund foundational research would make significant strides in improving the current models and informing future investment priorities. What is more, such research would have a profound impact well beyond government hiring and spending. Making this information available to the public would enable the whole of the economy to better understand and strengthen their cybersecurity workforce.

We cannot keep guessing when it comes to the cybersecurity workforce. Funding foundational research to answer these questions must be a priority.

Thank you for the opportunity to provide input. I hope that New America and I can continue to be a resource to the Subcommittee on this issue.