Equity and Diversity in the Nation’s Cyber Workforce

Policy Recommendations for Addressing Data Gaps

Irving Lachow

Introduction

U.S.-based businesses and government agencies face a shortage of between 350,000 and 600,000 cybersecurity professionals, and 56 percent of companies believe that their staffing shortfalls put them at moderate or extreme risk. Focusing on diversity, equity, and inclusion (DEI) can help organizations address that shortage by increasing the pool of available talent. Beyond the social good that comes with successful implementation of DEI policies, a 2018 McKinsey & Company report notes that organizations can also realize a positive impact on growth and performance. This is due to improved problem solving and idea generation: “Diverse teams have been shown to be more likely to radically innovate and anticipate shifts in consumer needs and consumption patterns—helping their companies to gain a competitive edge.” These benefits carry over to the cybersecurity realm. A diverse workforce can contribute to a better understanding of user behavior and the ever-evolving threat landscape. Additionally, diverse representation can help organizations identify and address implicit biases that may be impacting their ability to hire and retain talent, develop new products and services, and understand market demand across a broader demographic base.

MITRE recently conducted a study, funded by the Hewlett Foundation, that examined the current state of data on the diversity of the nation’s cyber workforce. The results of that study point to a data gap that needs to be addressed:

- There is not good data on the demographics of the cyber workforce, which makes it hard to assess how the United States is doing now. Without that baseline, it is not possible to accurately evaluate the effectiveness of different efforts attempting to increase the DEI of the workforce.
To address the lack of data, either the U.S. government (USG) or the philanthropic community should fund a yearlong dedicated pilot program run by a not-for-profit organization with the appropriate technical skills and the trust of both government and industry. This organization should develop and test multiple options for data gathering, analysis, and sharing. At the end of a year, the organization will share lessons learned and propose next steps.

In parallel to the pilot program, the USG should put in place the mechanisms needed to sustainably fund a multiyear initiative focused on the gathering, analysis, and dissemination of DEI cyber workforce data. The USG is the best solution for long-term funding for several reasons. First, the benefits of such an endeavor will support U.S. economic and security goals—a point that has been made by numerous senior government officials from both parties. Second, the USG is already heavily invested in growing the nation’s cyber workforce. Expanding its focus more heavily into the DEI aspects is a natural extension of its existing mission. Third, it will be difficult to find other funders for such an initiative. Philanthropy generally doesn’t fund open-ended efforts like this and industry likely won’t invest until it sees the benefits of doing so, which will take a few years.

This paper explores the specific steps that the USG could take to implement these recommendations. It examines which federal agency should take primacy on the funding and execution of a national DEI cyber workforce program. The paper also explores what other nations have done to address this topic. Finally, this paper examines the types of legislation that would be needed to make this program happen.

**Executive Branch Leadership**

Several federal agencies make good candidates for leading the charge on gathering, analyzing, and disseminating cyber workforce DEI data. The Commerce Department’s Bureau of Labor Statistics (BLS) is one option because it runs the Current Population Survey, which is a monthly survey of households that contains “a comprehensive body of data on the labor force, employment, unemployment, persons not in the labor force, hours of work, earnings, and other demographic and labor force characteristics.” Unfortunately, at the present, BLS only gathers data on one cyber-related job category: information security analyst. In addition, BLS’s information on this job category does not include demographic data. In theory, BLS could expand its survey methodology to gather information, including demographic data, for the full range of cyber jobs outlined in the National Initiative for Cybersecurity Education Workforce (NICE) Framework for Cybersecurity (which identifies 7 different categories, 33 specialty areas, and 52 different cyber roles). However, there is another federal agency that appears to be better positioned to gather demographic data specifically tied to the cyber workforce: the National Science Foundation (NSF).

The NSF’s National Center for Science and Engineering Statistics (NCSES) collects data on the United States’ science, technology, engineering, and mathematics (STEM) workforce, and it has a history of gathering demographic information. For example, it recently produced the report Women, Minorities, and Persons with Disabilities in Science and Engineering. In addition, the idea of expanding the NCSES’s remit to focus specifically on the cyber workforce has already been proposed in legislation. Both the National Science Foundation for the Future Act (H.R. 2225) and the America COMPETES Act of 2022 (H.R. 4521) direct the NSF director—working in cooperation with the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Defense, the Office of Personnel Management, and other federal agencies as required, to award grants to institutions of higher education or nonprofits to carry out research on the cyber workforce that includes analysis of demographic representation.
Another option worth mentioning is the Bureau of Cyber Statistic (BCS). The BCS concept was proposed by the Cybersecurity Solarium Commission, and it appears to be under active exploration by the Biden administration. While the primary focus of the BCS is to better understand risks and the efficacy of federal programs, the Solarium Commission report notes that the BCS could be used to collect, process, analyze, and disseminate statistical data on the “cyber ecosystem.” One could make the case that understanding the demographic posture of the nation’s cyber workforce is a key characteristic of that ecosystem. To that end, the proposed BCS could potentially play a role in gathering cyber workforce data if it were authorized, funded, and staffed to do that work. The question is whether the BCS should take this on when agencies like NSF are already well positioned for that task.

**Lessons from Other Countries**

What lessons can be learned from other countries? While several foreign governments, most notably Australia and New Zealand, are making concerted efforts to increase the diversity of their respective national workforces, the only nation pursuing the type of cyber workforce data gathering that this report proposes is the United Kingdom. In fact, the United Kingdom’s new cyber strategy specifically addresses the diversity of its cyber workforce. More to the point, over the last two years, the British government has performed surveys to “strive for a better understanding of the . . . diversity profile across the UK cyber security industry.” The United Kingdom’s approach follows the “Split the Difference” model that was proposed in the MITRE paper with one key difference: the UK government chose to work with a private-sector entity to gather and analyze cyber workforce data. The UK government also follows the paper’s recommendation that the data gathering be performed regularly over time. The lead organization for the effort is the National Cyber Security Center, a multiagency organization that includes elements from the intelligence community, law enforcement, and the British equivalent of DHS.

Adapting the British approach to the United States would put the Joint Cyber Defense Collaborative (JCDC) at the epicenter for the cyber workforce DEI initiative. According to its website, the JCDC brings together public- and private-sector partners that possess relevant equities in cyber defense operations to coordinate cybersecurity planning, information sharing, and information product and guidance development. . . . The JCDC’s federal government partners include representatives from the Department of Homeland Security (DHS), the Department of Defense (DoD), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI). The JCDC also consults with SLTT [state, local, tribal, and territorial] governments, information sharing and analysis organizations and centers (ISAOs/ISACs), owners and operators of critical information systems, cybersecurity researchers and subject matter experts, international partners, and other entities, as appropriate.

The JCDC is not well suited to lead a program focused on gathering, analyzing, and disseminating diversity data on the nation’s cyber workforce. While the JCDC emphasizes both public-private partnerships and information sharing, its primary orientation is operational. Other government agencies that focus on statistics are better suited to the role needed for this specific mission.

While the USG could adopt the British approach of working with a private-sector firm to conduct the data gathering, analysis, and dissemination, the use of a not-for-profit organization would help it avoid both real and perceived conflicts of interest. Fortunately, the United States has a rich network of not-for-profit organizations and industry associations with the expertise to do the work—
including some types that do not exist in the United Kingdom, such as federally funded research and development centers and university-affiliated research centers.

**Recommendations**

The research that MITRE conducted on behalf of the Hewlett Foundation, which included workshops and interviews, yielded the insight that neither the private sector nor the philanthropic community are likely to fund a yearslong effort to better understand the demographics of the cyber workforce in a detailed and comprehensive way. The U.S. federal government is the best option for taking this on and producing a public good that will benefit the nation as a whole.

There are several legislative options for enacting the type of program proposed in this paper. As mentioned above, both H.R. 2225 and H.R. 4521 propose that the NSF to gather demographic data on the nation’s cyber workforce. The latter bill has a greater chance of becoming a law, as it is the companion legislation to the United States Innovation and Competition Act (S. 1260) that was passed by the Senate. The Senate bill has several provisions aimed at increasing the diversity of the nation’s STEM workforce. Most of these provisions propose specific programs and activities (e.g., grants, apprenticeships). However, Section 308 calls for the creation of an interagency working group, led by the Office of Science and Technology Policy, to “compile and summarize available research and best practices on how to promote diversity and inclusions in STEM fields and examine whether barriers exist to promoting diversity and inclusion within federal agencies employing scientists and engineers.” Current language calls for the working group to “solicit and consider input and recommendations from non-federal stakeholders,” but does not provide a mandate or funding for this process.

The House and Senate are planning to reconcile the differences between H.R. 4521 and S. 1260 in committee. This presents the Hill with an opportunity to incorporate the language from the House bill into the final version of the legislation. Whatever wording is chosen, the proposed language should direct NSF to take the lead on this program with support from other key agencies like DHS and NIST.

Finally, the Executive Office of the President should actively support the goals of this proposed effort. The White House has already demonstrated that it cares about the issues of diversity and workforce. By using the power of the bully pulpit to indicate its support for the creation of a more diverse and equitable national cyber workforce, the White House may be able to encourage greater industry participation in the data-gathering activities that are so desperately needed.

Irving Lachow is a senior associate (non-resident) with the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2022 by the Center for Strategic and International Studies. All rights reserved.