Director of National Intelligence Dan Coats recently labeled cybersecurity his “greatest concern,” ahead of weapons of mass destruction and terrorism. While growing cybersecurity threats have far-reaching implications for national security, these concerns are also playing out on a daily basis for the many businesses and government agencies struggling to defend themselves against data breaches, denial of service attacks and ransomware. And one of the biggest challenges that organizations face as they try to keep up with the growing number of cyberattacks is finding workers with the right skills.

The cybersecurity skills shortage has been a long-standing problem for industry. In 2015, market research firm Frost & Sullivan estimated that there would be a 1.5 million global shortage of cybersecurity professionals by 2020. But this shortfall will continue to grow. Based on current trends, the International Information System Security Certification Consortium estimates that there will be a global shortage of 1.8 million workers by 2022.

The shortfall will have a significant impact on the United States. Every year, there are 40,000 U.S. cybersecurity jobs that go unfilled. CyberSeek, a project sponsored by
the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, estimates that there were 285,000 cybersecurity job openings in March 2018. Moreover, according to the Cisco 2018 Annual Cybersecurity Report, persistent staff shortages contribute to organizations failing to implement many important cybersecurity capabilities, such as multifactor authentication, network and endpoint forensics, and intrusion prevention systems.

Some states are addressing this problem head on. In Georgia, Gov. Nathan Deal announced last year that the state would spend $93 million to build a cyber innovation and training center in Augusta. The center will not only be an incubator for new cybersecurity startups and house the Georgia Bureau of Investigation’s cybercrime unit, but it will also provide space for cyberworkforce development programs, including training space for state and local professionals.

In Massachusetts, Gov. Charlie Baker announced in September 2017 the formation of the Cybersecurity Growth and Development Center. The new center will be part of the Massachusetts Technology Collaborative, an organization designed to grow the state’s technology sector. The center builds off of the state’s previous investment of $5 million in grants to local universities to establish new cybersecurity courses.

In Virginia, former Gov. Terry McAuliffe launched Cyber Vets Virginia in 2016, a cybersecurity training program to get more veterans to fill the vacant cybersecurity jobs in the state. The program partners with private-sector companies, such as Cisco and Amazon Web Services, to offer free training to veterans living in Virginia and helps place those who complete the training transition into a new occupation.

In 2017, Ohio Gov. John Kasich created the Ohio Cyber Collaboration Committee (OC3), a joint initiative of 30 public, private, military and educational organizations. The OC3’s mission is to increase the number of students pursuing cybersecurity certificates and degrees. To assist with this effort, OC3 has developed a “cyber-range” — a virtual environment for cybersecurity training. In December 2017 the OC3’s cyber-range held its inaugural event, a capture-the-flag challenge for Ohio high school and college students.

Finally, seven states recently partnered with the SANS Institute, a computer security research and training organization, to pilot the CyberStart program — a free online game that teaches high school students to complete various cybersecurity challenges. In total, 3,450 students participated in the competition, and top-ranked participants in each state won grants and scholarships to obtain additional cybersecurity training. This year, the SANS Institute launched Girls Go CyberStart, a similar program available in 16 states to recruit high school girls to the cybersecurity profession. These programs are important because many students do not consider cybersecurity as a potential career path. Three-quarters of women and two-thirds of men say that no high school teacher or guidance counselors mentioned cybersecurity as a profession.

Each of these programs offers lessons for other states on how to increase the supply of cybersecurity professionals. Finally, underlying these efforts should be significant
reforms to U.S. high schools and colleges to spur more and better computer science education.

http://www.govtech.com/data/Boosting-the-Cyberworkforce.html