U.S. HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HEARING CHARTER

More Hires, Fewer Hacks: Developing the U.S. Cybersecurity Workforce

February 11, 2020
10:00 a.m.
2318 Rayburn House Office Building

PURPOSE

On Tuesday, February 11, 2020 at 10:00 am, the Subcommittee on Research and Technology of the Committee on Science, Space, and Technology will hold a hearing to explore the challenges faced by organizations in both the public and private sectors in recruiting and training skilled cybersecurity professionals and discuss strategies to expand and diversify the cybersecurity workforce pipeline to meet the demand. The Committee will also assess the federal programs designed to address this workforce shortage.

WITNESSES

- **Mr. Rodney Petersen**, Director, National Initiative for Cybersecurity Education, National Institute of Standards and Technology
- **Dr. Ambareen Siraj**, Professor, Computer Science and Director, Cybersecurity Education Research and Outreach Center, Tennessee Tech University
- **Mr. Joseph Sawasky**, President and Chief Executive Officer, Merit Network, Inc.
- **Ms. Sonya Miller**, HR Director, IBM Security and Enterprise & Technology Security

KEY QUESTIONS

- What are the major challenges that have led to the cybersecurity workforce shortfall?
- How can we improve cybersecurity teaching and learning across all levels of education?
- What are effective pathways to prepare cybersecurity professionals for the workforce?
- How can we increase diversity, equity, and inclusion within the cybersecurity workforce?
- Where should Congress focus future efforts to bolster the cybersecurity workforce?

BACKGROUND

Cybersecurity is a highly skilled field that constantly evolves as cyber and cyberphysical systems grow increasingly interconnected and malicious actors exploit novel attack surfaces. However, education and training institutions have been unable to keep pace with the demand for cybersecurity graduates. As a result, organizations of all types face a persistent challenge in

recruiting and training cybersecurity professionals. According to CyberSeek, a tool funded by the National Initiative for Cybersecurity Education (NICE), there are over 500,000 job openings related to cybersecurity in the United States as of January 2020.[1] Similarly, a 2019 survey conducted by the International Information System Security Certification Consortium (ISC)² found that nearly 65 percent of organizations surveyed had a shortage of cybersecurity staff.[2] This shortage has resulted in intense competition for cybersecurity workers, which has disproportionally impacted public sector and nonprofit organizations that may lack the resources to compete with businesses for skilled hires.

There are many challenges to successfully training cybersecurity professionals. First, relatively few educational institutions focus on cybersecurity skills. For example, while computer science programs at colleges and universities often focus on high-level programming languages, such as Python, they often fail to teach low-level programming, such as C, that operate at the hardware and operating system level where most cybersecurity vulnerabilities are found.[3] At the K-12 education level, not only is there is a lack of STEM foundation, but few computer science courses at this level include cybersecurity components. At all education levels, there is a shortage of cybersecurity teachers able to train the students, which has contributed to this trend.

Second, the cybersecurity field lacks diversity, which contributes to fewer cybersecurity graduates. Research from Cybersecurity Ventures predicted that woman represented only 20 percent of the global cybersecurity workforce in 2019.[4] Furthermore, research conducted in 2018 by (ISC)² shows that while minority representation within cybersecurity is slightly higher than the overall U.S. minority workforce, "racial and ethnic minorities tend to hold non-managerial positions, with fewer occupying leadership roles, despite being highly educated."[5]

Third, some cybersecurity and education training programs fail to provide graduates with the skills and hands-on experience necessary to fill high-skilled technical cybersecurity roles. In 2018, the Department of Commerce and Department of Homeland Security (DHS) released a report that found employers were increasingly concerned about the relevance of cybersecurity-related education programs in meeting the needs of their organizations.[6] As a result, organizations are often required to provide additional on-the-job training for new hires. Furthermore, because cybersecurity is a rapidly developing field, employers must continuously maintain and enhance incumbent workers' skills.

The Federal government faces additional challenges in developing and maintaining a robust federal cybersecurity workforce, including rigidity of Federal pay systems, competition with higher-paying jobs in the private sector, opaque career paths, lengthy hiring and security

[1] "Cybersecurity Supply/Demand Heat Map." CyberSeek. January 2019.
[2] "(ISC)2 Cybersecurity Workforce Survey." International Information System Security Certification Consortium, 2019.
[3] William Crumpler and James A. Lewis, "A Cybersecurity Workforce Gap." The Center for Strategic and International Studies. January 2019.
[4] Steve Morgan. "Women Represent 20 Percent Of The Global Cybersecurity Workforce In 2019." Cybersecurity Ventures. March 28, 2019.
[5] "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce." International Information System Security Certification Consortium. 2018.
[6] "A Report to the President on Supporting Growth and Sustainment of the Nation's Cybersecurity Workforce." National Institute of Standards and Technology. May 2018.

clearance processes, and a lack of strategic plans to bolster agencies' cybersecurity workforce.[7] As a result, the federal government in particular has fallen behind in the race for skilled cybersecurity talent.

FEDERAL CYBERSECURITY WORKFORCE ACTIVITIES

Federal efforts to address the nationwide skill shortage in the public and private cybersecurity workforces having been growing over the last several years. Most recently, in May 2019, President Donald Trump issued an executive order to strengthen the federal cybersecurity workforce and the U.S. workforce pipeline more generally with coordination across the federal enterprise.[8] These efforts target the Federal cybersecurity education and training programs across several federal agencies, including the Department of Commerce, Department of Defense, Department of Energy, DHS, Department of Labor, and the National Security Agency (NSA). Federal programs span all stages of education, from elementary and secondary education to retraining programs for incumbent workers, and include activities such as cybersecurity-focused summer camps, academic competitions, scholarship and grant programs, and research on teaching and learning in cybersecurity fields.

NIST ACTIVITIES

The *Cybersecurity Enhancements Act of 2014* authorized the National Institute of Standards and Technology (NIST) to coordinate Federal support for cybersecurity education programs at all education levels and evaluate cybersecurity workforce needs. This bill codified the National Initiative for Cybersecurity Education (NICE), a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. NICE functions as a multi-stakeholder body, bringing together parties from across the public and private sector to develop and design cybersecurity workforce education, training, and workforce development. The Federal agencies communicate and coordinate among each other through the NICE Interagency Coordinating Council. The NICE Working Group brings together stakeholders from academia, private industry, and government to develop concepts, design strategies, and pursue actions that advance the initiative's goals. There are six subgroups within the Working Group, focused on apprenticeships, collegiate cybersecurity training, competitions, K-12 education, training and certifications, and workforce management. Each subgroup produces products, such as white papers, to advance education and workforce efforts in their domain.

In August 2017, NICE developed a framework that both categorizes cybersecurity jobs and describes the knowledge, skills, and abilities necessary to perform them.[9] The NICE Cybersecurity Workforce Framework groups common cybersecurity functions into categories based on common job functions, rather than job titles, subdividing these categories into specialty areas to identify specific knowledge and skills required to perform certain cybersecurity tasks.

---

[7] Kathryn Francis and Wendy Ginsberg. "The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security." Congressional Research Service. January 2016.
[8] "Executive Order on America's Cybersecurity Workforce." White House. May 2, 2019.
[9] William Newhouse et al. "National Initiative for Cybersecurity Education Cybersecurity Workforce Framework." National Institute for Standards and Technology. August 2017.

NICE has also pursued several other activities related to improving the cybersecurity workforce in the United States. For example, in 2019, NICE and several industry partners announced a tool called CyberSeek, which offers data about supply and demand in the cybersecurity job market.[10] In addition, NICE launched the Regional Alliances and Multistakeholder Partnerships program in 2016 to offer grants to develop regional and statewide consortia and communities to strengthen local cybersecurity workforce development.[11]

NSF ACTIVITIES

The National Science Foundation (NSF) funds several programs to bolster the cybersecurity workforce in the United States. First, the NSF Advanced Technological Education (ATE) program, which has awarded grants since 1994, supports educating high-skilled technicians across many disciplines, including cybersecurity.[12] NSF established three ATE Centers to lead development and dissemination efforts in cybersecurity education. ATE Centers offer resources, such as educational materials, and provide professional development to ensure that college or university cybersecurity education programs meet government and industry standards.

In partnership with the U.S. Office of Personnel Management (OPM) and DHS, NSF also oversees the Scholarship for Service (SFS) program, also known as CyberCorps. The SFS program provides scholarships for cybersecurity undergraduate and graduate education. In return for this support, recipients agree to work for the U.S. government in a cybersecurity position for a period equal to the length of the scholarship. There are over 80 institutions participating in SFS.[13] The National Defense Authorization Act (NDAA) of 2018 updated this program with two additions. First, the law authorized NSF to develop and implement a Community College Cyber Pilot Program (C3P), which expands the SFS program to community colleges for bachelor's degree recipients or veterans of the Armed Forces.[14] Second, the law created a requirement that at least 80 percent of scholarship recipients be placed in an executive agency, with the remainder going to state, local or tribal governments, National Laboratories, and Federally Funded Research and Development Centers. Some universities and colleges have found it difficult to meet this requirement, and it remains unclear how the requirement will be enforced.

NSF has several other programs to bolster the cybersecurity workforce. In 2015, NSF awarded grants to establish the Catalyzing Computing and Cybersecurity in Community Colleges (C5), a nationwide network of community colleges that have met national standards in cybersecurity education.[15] Moreover, NSF and NSA cosponsor the GenCyber Program to offer free cybersecurity summer camps to K-12 students and teachers.[16]

---

[10] "Cybersecurity Supply/Demand Heat Map." CyberSeek. Accessed February 3, 2020.
[11] "Regional Alliances and Multistakeholder Partnerships to Stimulate." National Institute for Standards and Technology. January 9, 2017.
[12] "Advanced Technological Education (ATE)." National Science Foundation. Accessed January 23, 2020.
[13] "Students: Participating Institutions." CyberCorps. Accessed January 23, 2020.
[14] "Community College Cyber Pilot Program makes first awards." National Science Foundation. October 3, 2018.
[15] C5. Accessed January 23, 2020.
[16] GenCyber. Accessed January 23, 2020.

CENTERS FOR ACADEMIC EXCELLENCE IN CYBERSECURITY

The National Centers for Academic Excellence (CAE) in Cybersecurity program, jointly sponsored by the NSA and DHS, encourage colleges and universities with cybersecurity degrees to meet certain academic standards for cybersecurity.[17] The goal of this program is to standardize cybersecurity education, training, and workforce development, promote higher education and research in cybersecurity, and produce professionals with cybersecurity expertise. The program was started in 1999 for universities, and in 2010, the NSA and DHS added a CAE2Y designation for regionally accredited two-year community colleges, technical schools, and government cybersecurity training centers. As of February 2020, the program has over 300 institutions with designations in cyber defense, research, and cyber operations. In 2017, the NSA and DHS established the CAE National Resource Centers and CAE Regional Resource Centers to provide an infrastructure among CAE-designated schools in different geographic regions as well as offer mentoring, webinar support, information sharing, and other tools.

CYBERSECURITY COMPETITIONS

Federal agencies, both civilian and military, also offer a variety of cybersecurity competitions. Cybersecurity competitions are an effective tool for educating and developing a cybersecurity workforce, offering a venue where individuals or teams compete in a variety of cybersecurity activities designed to build skills across cybersecurity fields. Cybersecurity competitions serve several different functions in the development and education of the cybersecurity workforce. Competitions create an environment in which students can develop skills in several different cybersecurity disciplines as well as apply theoretical concepts to examples of real-world problems. Competitions give high school and college students the opportunity to interact with cybersecurity professionals, and employers the opportunity to recruit. In addition to Federal programs, there are cybersecurity competitions that are administered by non-government entities that cover several different cybersecurity disciplines. Some of these competitions are annual events while others are structured as ongoing competitions throughout the year.

THE HACKED ACT

In November 2019, Senators Roger Wicker (R-MS), Maria Cantwell (D-WA), John Thune (R-SD) and Jacky Rosen (D-NV) introduced the *Harvesting American Cybersecurity Knowledge Through Education Act of 2019* (*HACKED Act of 2019*).[18] The House Committee on Science, Space, and Technology is planning a bipartisan introduction of a companion to this bill. The *HACKED Act* aims to bolster cybersecurity education in the United States by strengthening and expanding existing activities at Federal agencies. In brief, the bill would –

- Codify NIST as the agency responsible for leading interagency coordination of cybersecurity education and workforce training programs;
- Expand SFS to allow for students to fulfill their service obligation as teachers;

[17] "Celebrating 20 Years with the Centers of Excellence in Cyber Defense." CAE Community. 2019.
[18] Harvesting American Cybersecurity Knowledge through Education Act (HACKED Act). S.2775. 115th Cong. (2019).

- Amend certain NSF and National Aeronautics and Space Administration's (NASA) education programs to include cybersecurity;
- Authorize NIST to support regional partnerships between local employers and educational institutions to fill local cybersecurity workforce needs;
- Require NIST to identify model career paths for cybersecurity roles, create tools for assessing the federal workforce's skills and capabilities, and develop guidelines for improving cybersecurity awareness of federal employees.