# MORE HIRES, FEWER HACKS: DEVELOPING THE U.S. CYBERSECURITY WORKFORCE

## HEARING

BEFORE THE

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

Tuesday, February 11, 2020

**Serial No. 116–67**

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
39–616PDF WASHINGTON : 2021

## COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. EDDIE BERNICE JOHNSON, Texas, *Chairwoman*

ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
SUZANNE BONAMICI, Oregon
AMI BERA, California,
*Vice Chair*
LIZZIE FLETCHER, Texas
HALEY STEVENS, Michigan
KENDRA HORN, Oklahoma
MIKIE SHERRILL, New Jersey
BRAD SHERMAN, California
STEVE COHEN, Tennessee
JERRY McNERNEY, California
ED PERLMUTTER, Colorado
PAUL TONKO, New York
BILL FOSTER, Illinois
DON BEYER, Virginia
CHARLIE CRIST, Florida
SEAN CASTEN, Illinois
BEN McADAMS, Utah
JENNIFER WEXTON, Virginia
CONOR LAMB, Pennsylvania
VACANCY

FRANK D. LUCAS, Oklahoma,
*Ranking Member*
MO BROOKS, Alabama
BILL POSEY, Florida
RANDY WEBER, Texas
BRIAN BABIN, Texas
ANDY BIGGS, Arizona
ROGER MARSHALL, Kansas
RALPH NORMAN, South Carolina
MICHAEL CLOUD, Texas
TROY BALDERSON, Ohio
PETE OLSON, Texas
ANTHONY GONZALEZ, Ohio
MICHAEL WALTZ, Florida
JIM BAIRD, Indiana
FRANCIS ROONEY, Florida
GREGORY F. MURPHY, North Carolina
VACANCY

## Subcommittee on Research and Technology

HON. HALEY STEVENS, Michigan, *Chairwoman*

DANIEL LIPINSKI, Illinois
MIKIE SHERRILL, New Jersey
BRAD SHERMAN, California
PAUL TONKO, New York
BEN McADAMS, Utah
STEVE COHEN, Tennessee
BILL FOSTER, Illinois

JIM BAIRD, Indiana, *Ranking Member*
ROGER MARSHALL, Kansas
TROY BALDERSON, Ohio
ANTHONY GONZALEZ, Ohio
VACANCY

# CONTENTS

**February 11, 2020**

## Opening Statements

## Witnesses:

# MORE HIRES, FEWER HACKS: DEVELOPING THE U.S. CYBERSECURITY WORKFORCE

**TUESDAY, FEBRUARY 11, 2020**

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
*Washington, D.C.*

The Subcommittee met, pursuant to notice, at 10:07 a.m., in room 2318 of the Rayburn House Office Building, Hon. Haley Stevens [Chairwoman of the Subcommittee] presiding.

# 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.

Chairwoman STEVENS. This hearing will come to order. Without objection, the Chair is authorized to declare recess at any time.

Good morning, and welcome to this hearing of the Subcommittee on Research and Technology to explore the major challenges that have led to our national cybersecurity workforce shortage and the programs underway to address that shortage. A sincere and very special welcome to our distinguished panel of witnesses for joining us here today, the effort and time you took to write your testimony and obviously share your expertise. We're all very much looking forward to hearing from you.

Almost every day, we hear news about security breaches, poor system design, and vulnerabilities disrupting businesses and individuals' lives. Part of the reason cybersecurity issues are so prevalent is that the demand for skilled cybersecurity professionals far exceeds the supply of those individuals. According to CyberSeek, a tool funded by the National Initiative for Cybersecurity Education (NICE), as of last month there are over a half a million job openings related to cybersecurity in the United States. That's job openings. That means nearly one in three cybersecurity jobs go unfilled.

There are many reasons for this workforce shortfall. Relatively few high school students have any exposure to computer science in the classroom, let alone cybersecurity. Even when students graduate from college with a degree in computer science, they often lack the cybersecurity skills and hands-on experience to fill job openings.

We also recognize and encourage the multiple pathways to careers in cybersecurity, including certification programs and apprenticeships. On Saturday, just this past Saturday, I held a town hall back in Michigan on special education. And one of the excellent resources that was highlighted was the Living and Learning Enrichment Center, a center for adults with disabilities that has also just recently partnered with Cisco and the Michigan Career and Technical Institute, to start a cybersecurity certification to train adults with disabilities that traditionally present barriers to employment.

In addition, the cybersecurity field as a whole lacks diversity, even more so than many other STEM (science, technology, engineering, and math) fields. The math is yet again simple. Last year, women accounted for only 20 percent of the global cybersecurity workforce, the global cybersecurity workforce. Women of color in cybersecurity jobs make on average $10,000 less than their male counterparts. We cannot address our current and future cybersecurity workforce needs without recruiting and retaining more women and minorities into the field.

All of our panelists have been leaders in addressing the diversity challenge, and we very much look forward to hearing about your efforts on that front.

It should not be a surprise that I'm excited to have NIST (National Institute of Standards and Technology) represented on this panel to talk about their leadership in building the government's and the Nation's cybersecurity workforce. Truly, NIST has been a leader in of course setting the standards, the platform, even reaching out to the Department of Defense and forming one of the first MOUs (memorandum of understanding) to set cybersecurity standards in the advanced manufacturing space.

The National Institute of Standards and Technology is also playing a critical role in cybersecurity workforce development across this National Initiative for Cybersecurity Education, NICE. We'll also discuss many of the important Federal programs at the National Science Foundation, the Department of Homeland Security, and other agencies designed to educate and train the next generation of cybersecurity professionals.

Finally, we will explore how partnerships between academia, industry, and Federal and State governments are working to improve our cybersecurity workforce, humming and collaborating, and working together. I am so proud to say that my home State of Michigan has helped to lead the way in developing education and training programs to equip our State's workforce, Michiganders, with the skills they need to pursue a career in cybersecurity.

Governor Gretchen Whitmer, and even her predecessor Governor Snyder, have implemented programs like the Governor's High School Cyber Challenge and Girls Go Cyber to give Michigan high schoolers experience in cybersecurity. We will hear about some of those efforts today.

I want to thank the witnesses for being here today to help us understand these challenges that organizations face, companies face to recruit a skilled cybersecurity workforce, effective education and workforce development programs designed to help these organizations meet cybersecurity workforce needs, and how Federal agencies such as NIST are partnering with industry, university, and States to have America lead the way. Thank you.

[The prepared statement of Chairwoman Stevens follows:]

Good morning and welcome to this hearing of the Subcommittee on Research and Technology to explore the major challenges that have led to our national cybersecurity workforce shortage and the programs underway to address that shortage. A special welcome to our distinguished panel of witnesses for joining us here today. I'm looking forward to hearing your testimony. Almost every day we hear news about security breaches, poor system design, and vulnerabilities disrupting businesses and individuals' lives. Part of the reason cybersecurity issues are so prevalent is that the demand for skilled cybersecurity professionals far exceeds the supply of those individuals.

According to CyberSeek, a tool funded by the National Initiative for Cybersecurity Education (NICE), as of last month there are over a half a million job openings related to cybersecurity in the United States. That means nearly one in three cybersecurity jobs go unfilled.

There are many reasons for this workforce shortfall. Relatively few high school students have any exposure to computer science in the classroom, let alone cybersecurity. Even when students graduate from college with a degree in computer science, they often lack the cybersecurity skills and hands-on experience to fill job openings.

We must also recognize and encourage the multiple pathways to careers in cybersecurity, including certification programs and apprenticeships. On Saturday, I held a town hall on special education in my district. One of the excellent resources we highlighted is the Living & Learning Enrichment Center, a center for adults with disabilities that has just partnered with Cisco and the Michigan Career & Technical Institute to start a cybersecurity certification to train adults with disabilities that traditionally present barriers to employment.

In addition, the cybersecurity field as a whole lacks diversity, even more so than many other STEM fields. The math is simple: Last year, women accounted for only 20 percent of the global cybersecurity workforce. Women of color in cybersecurity jobs make on average $10,000 less than their male counterparts. We cannot address our current and future cybersecurity workforce needs without recruiting and retaining more women and minorities into the field. All of our panelists have been leaders in addressing the diversity challenge, and I look forward to hearing about your efforts on that front.

It should not be a surprise that I am excited to have NIST represented on this panel to talk about their leadership in building the government's and the nation's cybersecurity workforce. The National Institute of Standards and Technology is playing a critical role in cybersecurity workforce development across the country through the National Initiative for Cybersecurity Education. We will also discuss many of the important federal programs at the National Science Foundation, the Department of Homeland Security, and other agencies designed to educate and train the next generation of cybersecurity professionals.

Finally, we will explore how partnerships between academia, industry, and Federal and state governments are working to improve our cybersecurity workforce.

I am proud to say that my home state of Michigan has led the way in developing education and training programs to equip Michiganders with the skills they need to pursue a career in cybersecurity. Governor Gretchen Whitmer, and her predecessor Governor Snyder, have implemented programs like the Governor's High School Cyber Challenge and Girls Go Cyber to give Michigan high schoolers experiences in cybersecurity. We will hear about some of those efforts today.

I want to again thank the witnesses for being here today to help us understand the challenges that organizations face to recruit a skilled cybersecurity workforce, effective education and workforce programs designed to help organizations meet cybersecurity workforce needs, and how Federal agencies, such as NIST, are partnering with industry, universities, and states to lead the way.

Chairwoman STEVENS. At this time, the Chair is now going to recognize Dr. Baird for an opening statement.

Mr. BAIRD. Good morning, Chairwoman Stevens, and thank you for holding this hearing today and giving us the opportunity to examine the challenges both public and private that we're facing in recruiting and training cybersecurity professionals. And I do very much appreciate and we all appreciate all of you witnesses being here today and taking the time out of your schedule to do that.

But with advances in technology and the growth in the Internet of Things come the new methods that foreign countries and cybercriminals can use to attack and access our networks. So Americans' information is vulnerable, and we will hear today there is a demand for trained cybersecurity experts to identify and defend against cyber attacks.

According to the data derived from job posting, the number of unfilled security jobs has grown by more than 50 percent since 2015. And by 2022, the global cybersecurity workforce shortage is projected to reach upwards of 1.8 million. That's just 2 years away, so it kind of gives us a clue how fast and how demand is increasing.

So well-trained professionals are essential to our ability to implement proven security techniques. Institutions of higher education are working to create and improve cyber education and training programs focused on ensuring that there are enough professionals to meet our needs.

I am very proud to say that Indiana—did you catch that? Indiana has several universities that are leading the way in cyber education and training. Purdue University, which is the home to the Nation's first computer science department, hosts the Center for Education and Research in Information Assurance and Security, which is CERIAS. CERIAS is one of the seven original programs designed as a National Center of Academic Excellence in Cyber Defense, sponsored by the Department of Homeland Security and the National Security Agency.

The Purdue program has produced 215 graduates with doctoral degrees in cybersecurity and 329 graduates with master's degrees in cybersecurity. Purdue University Northwest is home to another

Center for Academic Excellence for information assurance and cyber defense education. As of this fall, Purdue Northwest has more than 200 students enrolled in its cybersecurity major.

Indiana is also very lucky to have two Centers of Academic Excellence designed and designated as 2-year institutions: Moraine Valley Community College and Ivy Tech Community College. These programs help us meet the growing demand nationwide for cybersecurity professionals at all skill levels.

The Science Committee has an important role in supporting programs that are providing the skills and expertise needed to defend and support our systems from cyberthreats. I'm an original cosponsor to the *Securing American Leadership in Science and Technology Act*. This legislation takes important steps to improve America's cybersecurity capabilities. It makes strategic investments in cybersecurity research and development across Federal science agencies. And it supports building up the NSF (National Science Foundation) Scholarship for Service program, CyberCorps, to grow and improve the quality of America's cybersecurity workforce. Protecting America's cyber-systems is critical to our economic and national security.

While these Federal programs play an important role, industry has really stepped up and developed some initiative and innovative programs to address the cybersecurity skills gap that we are currently facing, such as IBM's New Collar program.

I would like to thank each of the witnesses for taking the time to be here, and we really appreciate your efforts and expertise. I look forward to hearing from each of you and provide an overview of the state of the cybersecurity workforce and recommend how the Federal Government can best work with industry and academia to meet this challenge.

Thank you, and I yield back the balance of my time.

[The prepared statement of Mr. Baird follows:]

Good morning Chairwoman Stevens and thank you for holding today's hearing to examine the challenges both the public and private sectors are facing in recruiting and training cybersecurity professionals.

With advances in technology and the growth of the "internet of things" come new methods that foreign countries and cybercriminals can use to attack and access our networks.

Americans' information is vulnerable and, as we will hear today, there is a demand for trained cybersecurity experts to identify and defend against cyber-attacks.

According to data derived from job postings, the number of unfilled cybersecurity jobs has grown by more than 50 percent since 2015. By 2022, the global cybersecurity workforce shortage is projected to reach upwards of 1.8 million unfilled positions.

Well-trained professionals are essential to our ability to implement proven security techniques. Institutions of higher education are working to create and improve cyber education and training programs focused on ensuring there are enough professionals to meet our needs.

I am very proud to say that Indiana has several universities that are leading the way in cyber education and training. Purdue University, which is home to the nation's first computer science department, hosts the Center for Education and Research in Information Assurance and Security (CERIAS).

CERIAS is one of the seven original programs designed as a National Center of Academic Excellence in Cyber Defense, sponsored by the Department of Homeland Security (DHS) and the National Security Agency (NSA).

The Purdue program has produced 215 graduates with doctoral degrees in Cybersecurity and 329 graduates with master's degrees in Cybersecurity. Purdue University Northwest is home to another Center of Academic Excellence for Information Assurance and Cyber Defense Education. As of this fall, Purdue Northwest has more than 200 students enrolled in its Cybersecurity major.

Indiana is also very lucky to have two Centers of Academic Excellence designated two-year institutions: Moraine Valley Community College and Ivy Tech Community College. These programs help us meet the growing demand nationwide for cybersecurity professionals at all skill levels.

The Science Committee has an important role in supporting programs that are providing the skills and expertise needed to defend and support our systems from cyberthreats.

I am an original co-sponsor of the Securing American Leadership in Science and Technology Act. This legislation takes important steps to improve America's cybersecurity capabilities. It makes strategic investments in cybersecurity research and development across federal science agencies. And it supports building up the NSF scholarship for service program, Cybercorps, to grow and improve the quality of America's cybersecurity workforce.

Protecting America's cyber-systems is critical to our economic and national security.

While these federal programs play an important role, industry has really stepped up and developed some innovative programs to address the cybersecurity skills gap we are currently facing, such as IBM's New Collar program.

I would like to thank each of our witnesses for taking the time to be here with us this morning. I look forward to hearing from you as you provide an overview of the state of the cybersecurity workforce and recommend how the federal government can best work with industry and academia to meet this challenge.

Thank you and I yield back the balance of my time.

Chairwoman STEVENS. Thank you. And at this time the Chair now recognizes our Chairwoman, Chairwoman Johnson of the full Science Committee, for an opening statement.

Chairwoman JOHNSON. Thank you very much, Chairwoman Stevens and Ranking Member Baird, for holding this morning's hearing on developing our Nation's cybersecurity workforce, and I want to welcome and thank our expert witnesses for their testimony as well.

We spend a lot of time in the Science, Space, and Technology Committee focusing on the challenges in developing a skilled STEM workforce for the 21st Century, and on exploring the ways in the which the Federal Government can best address these challenges. While we need to develop the STEM pipeline across all fields, there are particular fields in which the gap between the supply and demand is especially acute. Cybersecurity is one of those.

Technology alone will not mitigate the many risks that individuals, businesses, and governments face in cyberspace. We need researchers who understand the risks as they evolve and can build new defensive tools. We need executives who understand what is needed to defend their own organizations. We need technicians monitoring the systems on a daily basis. And we need many other types of cybersecurity jobs in between.

The fact is we need to educate and train individuals in cybersecurity at all levels, and it requires not just degrees but different types of certifications, as well as continuing education for those already in the workforce. And finally, we need the general public to be well-educated about cyber hygiene, starting in our elementary schools.

The National Initiative for Cybersecurity Education, or NICE, was created under the Obama Administration to coordinate and expand Federal investments in a skilled cybersecurity workforce and a cybersecurity-savvy public. Congress, led by this Committee, certified NICE in the *Cybersecurity Enhancement Act of 2013*.

The National Institute of Standards and Technology is tasked with leading NICE. NIST is not traditionally an agency that leads on workforce issues. It is, however, an agency that leads on cybersecurity standards for both the public and private sectors. With its unique understanding and unsurpassed expertise in cybersecurity, NIST is the right agency to coordinate to lead efforts to develop a cybersecurity workforce for the Nation.

The Science, Space, and Technology Committee has been enacting cybersecurity-focused legislation since 2002, and we are planning to move additional legislation this year. I look forward to continuing to collaborate across the aisle and across Committee lines to take a whole-of-government approach to cybersecurity, starting with the workforce.

In that regard, I look forward to hearing from today's witnesses in how the activities carried out under NICE can continue to be strengthened.

Thank you, and I yield back.

[The prepared statement of Chairwoman Johnson follows:]

Thank you Chairwoman Stevens and Ranking Member Baird for holding this morning's hearing on developing our nation's cybersecurity workforce and I want to welcome and thank the expert witnesses for their testimony.

We spend a lot of time in the Science, Space, and Technology Committee focusing on the challenges in developing a skilled STEM workforce for the 21st Century, and on exploring the ways in the which the Federal government can best address those challenges. While we need to develop the STEM pipeline across all fields, there are particular fields for which the gap between supply and demand is especially acute. Cybersecurity is one such field.

Technology alone will not mitigate the many risks that individuals, businesses, and governments face in cyber space. We need researchers who understand the risks as they evolve and can build new defensive tools. We need executives who understand what is needed to defend their own organizations. We need technicians monitoring the systems on a daily basis. And we need many other types of cybersecurity jobs in between. The fact is we need to educate and train individuals in cybersecurity at all levels, and it requires not just degrees but different types of certifications as well as continuing education for those already in the workforce. Finally, we need the general public to be well educated about cyber hygiene, starting in our elementary schools.

The National Initiative for Cybersecurity Education, or NICE, was created under the Obama Administration to coordinate and expand Federal investments in a skilled cybersecurity workforce and a cybersecurity savvy public. Congress, led by this Committee, codified NICE in the Cybersecurity Enhancement Act of 2013. The National Institute of Standards and Technology is tasked with leading NICE. NIST is not traditionally an agency that leads on workforce issues. It is, however, an agency that leads on cybersecurity standards for both the public and private sectors. With its unique and unsurpassed expertise in cybersecurity, NIST is the right agency to continue to lead efforts to develop a cybersecurity workforce for the nation.

The Science, Space, and Technology Committee has been enacting cybersecurity-focused legislation since 2002, and we are planning to move additional legislation this year. I look forward to continuing to collaborate across the aisle and across Committee lines to take a whole-of-government approach to cybersecurity, starting with the workforce.

In that regard, I look forward to hearing from today's witnesses how the activities carried out under NICE can continue to be strengthened.

Chairwoman STEVENS. Great, thank you, Madam Chair.

If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

And at this time I'd like to introduce our witnesses. Our first witness is Mr. Rodney Petersen. Mr. Petersen is the Director of the National Initiative for Cybersecurity Education, NICE, at the National Institute of Standards and Technology. Prior to his position at NICE, Mr. Petersen served as the Managing Director of the EDUCAUSE Washington office and Senior Government Relations Officer. He founded and directed the EDUCAUSE Cybersecurity Initiative and was the staff liaison for the Higher Education Information Security Council. Prior to joining EDUCAUSE, he worked two different times for the University of Maryland first as Chief Compliance Officer in the Office of the President and later as the Director of IT Policy and Planning in the Office of the Vice President and Chief Information Officer. Mr. Petersen is also the co-editor of a book entitled *"Computer and Network Security in Higher Education."*

Our next witness is Dr. Ambareen Siraj. Dr. Siraj is a Professor of Computer Science and the founding Director of Tennessee Tech University's Cybersecurity Education Research and Outreach Center, and has served as the leader on several NSF and NSA (National Security Agency) education and workforce development grants. Dr. Siraj is also the founder of the Women in Cybersecurity organization, an NSF-funded initiative to recruit, retain, and advance women in cybersecurity. Dr. Siraj's research focus is on security in cyber physical systems, Internet of Things, situation assessment and network security, security education and workforce development. She was a 2018 recipient of the Colloquium for Information System Security Education Exceptional Leadership in Education Award.

After Dr. Siraj is Mr. Joseph Sawasky. Mr. Sawasky is currently the President and CEO of Merit Network, a nonprofit corporation governed by Michigan's public universities. Merit owns and operates the Nation's longest-running regional research and education network, having been formed in 1966 by the University of Michigan, Michigan State University, and Wayne State University. Mr. Sawasky and his team at Merit also run the Michigan Cyber Range, the Nation's largest unclassified network-accessible cybersecurity training platform. Prior to his role at Merit, Mr. Sawasky was the Chief Information Officer at Wayne State University, doing this from 2007 to 2015, during which time he also served on the boards of the Merit Network, the Detroit CIO Executive Summit, and Michigan Technology Leaders. He also worked at the University of Toledo for 22 years and in his last position served as CIO. We are delighted we recruited him to Michigan.

Our fourth witness is Ms. Sonya Miller. Ms. Miller is the IBM H.R. Director for both IBM Security and Enterprise and Technology Security, two distinct divisions within IBM that require workers who have the skills and experience in cybersecurity to protect IBM and IBM clients. IBM Security has 8,000 employees, including researchers, developers, and subject matter experts focused on security and more than 10,000 security-related patents. Wow. Since 2015, IBM Security has hired nearly 4,400 additional experts into its security business. In her position, Ms. Miller is charged with ensuring both divisions have the skilled staff necessary to fulfill their missions. Wow. Just an absolute fantastic panel.

As our witnesses should know, each of you will have 5 minutes for your spoken testimony. Be sure to put your mic on. Your written testimony will be included in the record for the hearing. And when you've completed your spoken testimony, we'll begin with questions. Each Member will have 5 minutes to question the panel. And for testimony, we're going to start with Mr. Petersen.

## TESTIMONY OF MR. RODNEY PETERSEN, DIRECTOR, NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Mr. PETERSEN. Thank you, Chairwoman Stevens, Ranking Member Baird, and Members of the Subcommittee. I am Rodney Petersen, the Director of the National Initiative for Cybersecurity Education, or NICE, at the Department of Commerce's National Institute of Standards and Technology known as NIST. Thank you for the opportunity to appear before you today to discuss the role that NICE plays in interagency coordination for cybersecurity education workforce issues, and the challenges the Federal Government faces in recruiting and retaining skilled cybersecurity practitioners.

NICE is a partnership between government, academia, and the private sector. Our program is focused on promoting and energizing a robust network and ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with its partners to build on existing successful programs, facilitating change and innovation, and bringing leadership and vision to increase the number of skilled cybersecurity workers to keep our Nation secure.

To coordinate at the Federal level, NICE Interagency Coordinating Council convenes our Federal Government partners for consultation, communication, policy, and strategic direction. This coordination provides an opportunity for the NIST-led NICE program office to communicate program updates with key partners in the Federal Government, as well as to learn about other Federal Government activities in support of NICE. The group also identifies and discusses policy issues and provides input into the strategic directions for NICE.

Another means of coordination is the NICE working group. This working group has been established to provide a mechanism in which the public and private sector participants can develop concepts, design strategies, pursue actions that advance cybersecurity education, training, and workforce development.

Let me share a couple of accomplishments from our current NICE strategic plan. First, NICE issued six awards to pilot Regional Alliances and Multi-stakeholder Partnerships Stimulating Cybersecurity Education and Workforce Development. These regional communities, known as RAMPS for cybersecurity workforce, were designed to stimulate local economic communities to work together to rally education and training providers to meet local workforce needs.

Second, NICE also awarded a grant to develop a website known as CyberSeek that was cited earlier today, which includes both an interactive jobs heat map, as well as a career pathway portal. The jobs heat map shows that there are over 500,000 open jobs in cybersecurity today across the United States. It further indicates that there are almost a million people employed in cybersecurity today. The map can be used to search for demand by State. For example, there are 8,760 open positions in Michigan alone, 5,603 in

Tennessee, and 4,533 in Indiana. You can also use that website to search by major metropolitan areas either within a State or across State lines. So, for example, the D.C. metropolitan area in which we currently reside has 64,089 open jobs.

One of the challenges in cybersecurity education training and workforce development is having a common language. To meet this need, NIST published the NICE Cybersecurity Workforce Framework. The common taxonomy in the NICE framework can be used by employers to structure their workforce, develop position descriptions, or craft employee development plans. The NICE framework begins to demystify a career in cybersecurity by showing the variety of types of work roles that exist and the multiple career pathways for entering and advancing in a cybersecurity career. An update to that NICE framework is happening this year.

During 2020, NICE is embarking upon a consultative process that will result in a new 5-year strategic plan, as required by the Cybersecurity Enhancement Act, and that plan will be informed by the community that we serve.

As NICE develops its next strategic plan, a few trends are beginning to emerge. First, the need to enhance cybersecurity career discovery for learners of all ages. Second, the need to transform the learning process to emphasize the multidisciplinary nature of cybersecurity and the multiple pathways to enter into a cybersecurity career. And third, the need to modernize the talent acquisition process to facilitate skills-based hiring that enables career mobility.

All of these trends and current activities of NICE directly support the goals of the National Council for the American Worker. Established under Executive Order, the National Council is creating the first-ever national workforce strategy. This strategy is promoting the importance of multiple pathways to careers, the central role that employers play as part of our national education and workforce system, the need for companies to employ skill-based hiring, the need for greater transparency in the skills that companies need, and the return on investment of different learning pathways.

NIST is excited about the accomplishments of the NICE program in addressing the future of cybersecurity education in the United States in order to increase the number of skilled cybersecurity practitioners that are helping to keep our Nation secure. NIST looks forward to continuing to support the Nation's ability to address current and future challenges through standards and best practices.

Thank you for the opportunity to testify today, and I would be happy to answer any questions that you may have.

[The prepared statement of Mr. Petersen follows:]

Testimony of

Rodney Petersen

Director, National Initiative for Cybersecurity Education (NICE)
National Institute of Standards and Technology
U.S. Department of Commerce

Before the

Subcommittee on Research and Technology of the
Committee on Science, Space, and Technology
United States House of Representatives

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

February 11, 2020

**Introduction**

Chairwoman Stevens, Ranking Member Baird, and Members of the Subcommittee, I am Rodney Petersen, Director of the National Initiative for Cybersecurity Education (NICE) program at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss NIST's National Initiative for Cybersecurity Education (NICE) program, the role NICE plays in interagency coordination for cybersecurity workforce pipeline issues and the challenges the federal government faces in recruiting and retaining skilled cybersecurity professionals.

**NICE**

Home to five Nobel Prizes, with programs focused on national priorities such as advanced communications, artificial intelligence, quantum science, advanced manufacturing and biosciences, NIST's mission promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In support of this mission, the National Initiative for Cybersecurity Education (NICE), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development aimed at energizing and promoting a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with its partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity workers helping to keep our Nation secure.

2019 marked a year of milestones for the cybersecurity education and workforce development movement in the United States. In November, the 10th annual NICE Conference and Expo was held in Phoenix, Arizona. In December, NICE held the 5th annual NICE K-12 Cybersecurity Education Conference in Anaheim, California. Throughout 2019, NICE recognized the accomplishments resulting from 20 years of the National Centers of Academic Excellence in Cybersecurity. These milestones during 2019 allowed the NICE program to celebrate the work that has been accomplished to date and look forward to the future – the next 5 years, decade, or 20 years – to aspire to even greater improvements and innovations. While many consider the cybersecurity workforce gap a challenge, the NIST partnership looks at it as an opportunity and the NICE community is laser focused on addressing education and workforce problems with innovative solutions.

**Consultative Process**

The NICE Interagency Coordinating Council (ICC) convenes federal government partners of NICE for consultation, communication, and coordination of policy initiatives and strategic directions related to cybersecurity education, training, and workforce development. The meetings provide an opportunity for the NIST-led NICE Program Office, to communicate program updates with key partners in the federal government and to learn about other federal government activities in support of NICE. The group also identifies and discusses policy issues and provides input into the strategic directions for NICE.

The NICE Working Group has been established to provide a mechanism in which ***public*** and ***private*** sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. The working group is further divided into six sub-working groups focused on:

- K12 Education
- Collegiate Education
- Training and Certifications
- Competitions
- Apprenticeships
- Workforce Management

**NICE Strategic Plan**

The Cybersecurity Enhancement Act of 2014 authorized NICE and requires a strategic plan to be updated and submitted to Congress every five years. During 2020, NICE is embarking upon a consultative process that will result in a new 5-year strategic plan that is informed by the community that we serve.

The 2016 NICE Strategic Plan includes the following goals:

- Accelerate Learning and Skills Development - *Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers*
- Nurture a Diverse Learning Community - *Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce*
- Guide Career Development and Workforce Planning - *Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent*

Each of these goals are supported by objectives, tactics, and measures of success.

As an example, one of the objectives in the NICE Strategic Plan is to "facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs" which is why NIST issued a Federal Funding Opportunity to pilot six Regional Alliance and Multi-stakeholder Processes Stimulating (RAMPS) Cybersecurity Education and Workforce Development. NIST received over 60 applications from almost 40 different states. The selected RAMPS communities were employer-led, learner-centered, community-oriented, standards-based, and outcomes-driven. The pilots were held in local economic communities in five different states. A *Roadmap for Successful RAMPS Regional Alliances and Multi-stakeholder Partnerships to Build the Cybersecurity Workforce* has been published as a NIST Informational Resource that identifies the challenges and successes of the RAMPS pilot.

As another example of an objective in the strategic plan, NICE sought to "identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers." The "forecasting of future cybersecurity workforce needs" was specifically directed in the Cybersecurity Enhancement Act which is why NICE awarded a grant to CompTIA and Burning Glass to develop the website known as CyberSeek - www.CyberSeek.org - that includes both an interactive heat map as well as a cybersecurity career pathway portal. The jobs heat map is updated periodically and currently reflects that as of November 2019 there are 504,316 open jobs in cybersecurity across the United States. It further indicates that there are 997,058 individuals employed in cybersecurity. The map can be searched for cybersecurity workforce demand by state. For example, there are 8,760 open cybersecurity jobs in Michigan, 5,603 in Tennessee, and 4,533 in Indiana. One can also determine the workforce demand by major metropolitan area within a state or across state boundaries. For example, the DC Metropolitan area includes 64,089 open jobs.

**NICE Cybersecurity Workforce Framework**
One of the challenges in cybersecurity education, training, and workforce development is the need to be speaking the same language and having the same reference point for cybersecurity. That is why NIST as a standards organization was well positioned to publish the NICE Cybersecurity Workforce Framework -- NIST Special Publication 800-181. The NICE Framework provides a common taxonomy or lexicon for describing cybersecurity work. It is a reference resource that can be used by employers in both the public and private sectors to structure their workforce, including the development of positions descriptions, identification of training and development needs of employees as part of performance management plans, and the description of career pathways for both the incoming and current workforce. The NICE Framework also contains detailed task descriptions and knowledge, skills, and abilities statements that education and training providers can use to ensure that they are developing the workforce that employers need. For students or job seekers, it begins to demystify a career in cybersecurity by showing the variety of types of work roles that exist and the multiple career pathways for entering into and advancing in a cybersecurity career.

The program is currently embarking upon a review and update of the NICE Framework during 2020 to ensure that it remains relevant for all of the stakeholders – from employers to learners to educators and training providers – and to capture the different applications and uses of the NICE Framework. NIST announced a Request for Comments in November of 2019 and is currently reviewing the input received. NIST will engage in a consultative process to further engage stakeholders in an effort to improve the next draft of the NICE Framework. In addition to our interests to continuously improve the NICE Framework, the Executive Order on America's Cybersecurity Workforce requires the Secretary of Commerce to provide annual updates to the President regarding effective uses of the NICE Framework by non-Federal entities and make recommendations for improving the application of the NICE Framework in cybersecurity education, training, and workforce development.

The Federal Cybersecurity Workforce Assessment Act of 2015 requires the Federal Government to use the NICE Framework to assess its cybersecurity workforce and identify gaps in areas of critical need. The Executive Order on America's Cybersecurity Workforce will also extend use of the NICE Framework to federal contractors. Additionally, the executive order directs the

Secretaries of Commerce, Labor, Education, and Homeland Security, as well as the heads of other appropriate agencies, to "encourage the voluntary integration of the NICE Framework into existing education, training, and workforce development efforts undertaken by State, territorial, local, tribal, academic, non-profit, and private-sector entities, consistent with applicable law." The implementation of the Executive Order is in progress.

**Growing and Sustaining the Nation's Cybersecurity Workforce**
In 2017, the Department of Commerce and Department of Homeland Security delivered a report to the president entitled, "Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future".[1] The report was developed in response to Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructures that directed the Secretary of Commerce and Secretary of Homeland Security to:

1) "assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education"; and,

2) "provide a report to the President ...with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors."

The report sets forth a vision to "prepare, grow, and sustain a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity" and identifies four imperatives along with a corresponding set of recommendations and actions:

- Imperative 1: Launch a national Call to Action to draw attention to and mobilize public and private sector resources to address cybersecurity workforce needs.
- Imperative 2: Transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce.
- Imperative 3: Align education and training with the cybersecurity workforce needs of employers and prepare individuals for lifelong careers.
- Imperative 4: Establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

In May of 2019, the America's Cybersecurity Workforce Executive Order directed the Secretary of Commerce and the Secretary of Homeland Security, in coordination with the Secretary of Education and the heads of other agencies, to "execute, consistent with applicable law and to the greatest extent practicable, the recommendations from the report[.]"

**Looking Ahead**
As NICE develops its strategic plan for the next five years, a few trends continue to emerge: the need to enhance cybersecurity career discovery for learners of all ages, transform the learning process to emphasize the multidisciplinary nature of cybersecurity and the multiple career

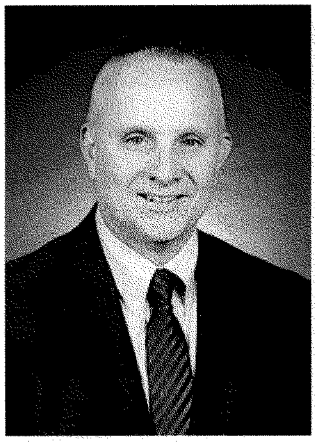
[1] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/report

pathways, and modernize the talent acquisition process to facilitate skills-based hiring and career mobility. All of these trends and the current activities of NICE directly support the goals of the National Council for the American Worker, which Secretary Ross co-leads with Advisor Ivanka Trump. Established under Executive Order, the National Council is creating the first ever national workforce strategy. This strategy is promoting the importance of multiple pathways to careers (not just a 4-year university education), the essential role of employers as part of our national education and workforce system, the need for companies to employ skill-based hiring and the need for greater transparency in the skills that companies need and the return on investment of different educational pathways.

**Conclusion**

NIST is excited about the accomplishments of the National Initiative for Cybersecurity Education program in addressing the future of cybersecurity education in the U.S. in order to increase the number of skilled cybersecurity professionals helping to keep our Nation secure. NIST looks forward to continuing to support the country's ability to address current and future cybersecurity challenges through standards and best practices.

Thank you for the opportunity to testify today. I would be happy to answer any questions that you may have.



**Rodney Petersen**
**Director of the National Initiative for Cybersecurity Education (NICE)**

Rodney Petersen is the Director of the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. He previously served as the Managing Director of the EDUCAUSE Washington Office and a Senior Government Relations Officer. He founded and directed the EDUCAUSE Cybersecurity Initiative and was the lead staff liaison for the Higher Education Information Security Council. Prior to joining EDUCAUSE, he worked at two different times for the University of Maryland - first as Campus Compliance Officer in the Office of the President and later as the Director of IT Policy and Planning in the Office of the Vice President and Chief Information Officer. He also completed one year of federal service as an Instructor in the Academy for Community Service for AmeriCorps' National Civilian Community Corps. He is the co-editor of a book entitled "Computer and Network Security in Higher Education". He received his law degree from Wake Forest University and bachelor's degrees in political science and business administration from Alma College. He was awarded a certificate as an Advanced Graduate Specialist in Education Policy, Planning, and Administration from the University of Maryland.

## TESTIMONY OF DR. AMBAREEN SIRAJ, PROFESSOR, COMPUTER SCIENCE, AND DIRECTOR, CYBERSECURITY EDUCATION RESEARCH AND OUTREACH CENTER, TENNESSEE TECH UNIVERSITY

Dr. SIRAJ. Chairwoman Stevens, Ranking Member Baird, and the Members of the Committee and Subcommittee, thank you for inviting me today in this very important discussion. My name is Ambareen Siraj. I was born and raised in Bangladesh where my dad taught me two simple things: working hard and serving others. I'm blessed that this Nation has provided me, an underrepresented immigrant, with an opportunity to serve as an educator, a researcher, and a leader.

I'm honored to share with you today how we at Tennessee Tech are contributing to the development of the U.S. cybersecurity workforce. Reputed statewide for its undergraduate engineering education, Tennessee Tech is located in the city of Cookeville in middle Tennessee with a student population of a little over 10,000. Our computer science, C.S., enrollment is increasing at a higher rate than any College of Engineering programs. Among the three focus areas in C.S., cybersecurity has the majority of students, around 500, and its enrollment quadrupled in the last 4 years since it started.

Operating since 2016, CEROC (Cybersecurity Education, Research and Outreach Center) is a Center of Academic Excellence in cyber defense education accredited by the National Security Agency and the Department of Homeland Security. At CEROC our cybersecurity students, we facilitated an integrated experience in informal education, research, and outreach activities alongside their formal cybersecurity education as part of the C.S. curriculum. With the mantra of continuous learning, crowd-sourced learning, and playing it forward, our students are constantly challenged to immerse themselves into educational experiences that enrich self and those around them.

Over the last few years multiple CEROC projects funded through the National Science Foundation and the Department of Defense have impacted thousands of secondary and postsecondary students and hundreds of educators in Tennessee and beyond. Scholarship for Service (SFS), DOD CySP, and GenCyber are among these.

One of our programs with great impact is the Women in Cybersecurity (WiCyS) initiative. At the time when female representation of cybersecurity was only 11 percent, our journey began in 2013 with funding from National Science Foundation. Today, I'm proud to let you know that over 7 years and $3.5 million funding from industry support WiCyS has provided approximately 3,000 student scholarships, 340 faculty scholarships, and 6,400 in attendance. Not only the flagship conference for women in cyber, WiCyS has become, regardless of gender, the largest security conference in the Nation that ensures comparable representation of students and professionals in the audience both from public and private sectors.

Operating as a nonprofit organization since late 2017, WiCyS is more than 6,000 members strong with 89 student chapters across 35 States, 15 professional affiliates across 20 States, and a suite of services to its community that includes students, professionals, educators, and veterans.

There is yet a lot to be done. The current 20 percent female representation in cybersecurity is not just a threat to diversity and inclusion but also a threat to the cybersecurity workforce pipeline. To bolster the cybersecurity workforce, I encourage Congress to invest in Federal programs such as CAE (Center for Academic Excellence), SFS (Scholarship for Service), CySP, GenCyber, and commission more of such programs that enable educational and nonprofit programs to support diverse populations in cyber, community college pathways, preparation and pipeline of educators, and nontraditional pathways for workers. The support opportunities and resources provided by these Federal grants are central to enable smaller schools like us to contribute in the Nation's cyber agenda in our own ways with our own strength and through our own community and beyond.

As we continue to do our part, I would like to end with a quote from one of our many students at Tennessee Tech who are hardworking, humble, and optimistic about their future and their country. M. writes, "This program has given me the courage to dream big, to continue seeking knowledge, and to make a difference in the world."

I sincerely appreciate the opportunity to speak today. I hope that Tennessee Tech, CEROC, and I can continue to be a resource for Congress. I look forward to our discussion. Thank you.

[The prepared statement of Dr. Siraj follows:]

CEROC
Cybersecurity Education,
Research and Outreach Center

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

A Hearing before the Subcommittee on Research and Technology,
House Committee on Science, Space and Technology
Congressional Testimony
by

Dr. Ambareen Siraj
Professor, Computer Science
Director, Cybersecurity Education, Research and Outreach Center
Tennessee Tech University
February 11, 2020

## About Us

Chairwoman Stevens, Ranking Member Baird, and the esteemed members of the Committee and the Subcommittee, thank you for inviting me to speak on the topic of developing the U.S. cybersecurity workforce. I am humbled and honored to participate in this very important discussion.

My name is Ambareen Siraj. I was born and raised in Bangladesh where my father taught me two simple things: working hard and serving others. I came here to pursue an advanced degree in Computer Science in 1997. I am blessed that this nation has provided me - an under-represented immigrant, with an opportunity to serve as an educator, a researcher, and a leader. I am Professor of Computer Science and Founding Director of the Cybersecurity Education, Research and Outreach Center (CEROC) at Tennessee Tech University. I am also the Founder of the Women in CyberSecurity, a.k.a., WiCyS conference and organization. Today I am honored to share with you how we, at Tennessee Tech University, are playing our role in the advancement of cyber workforce in our state, our region and the nation.

My testimony will solely focus on our actions at Tennessee Tech and my recommendations for federal assistance in developing U.S. cybersecurity workforce. I will refrain from referring to widely known statistics that clearly emphasize the importance of this hearing today. The most important statistic that should guide this discussion is the fact that there will be 3.5 million unfilled cybersecurity jobs globally by next year[1]; currently, as we speak, there are more than half million jobs open in the nation[2].

Tennessee Tech University[3] is located in the city of Cookeville in Putnam County, Tennessee, with a population of 31,004 in the city and 75,931 in the county. Although the county is known for its relative economic strength and concentration of academic and industrial resources, the areas of the Upper Cumberland region that surround Putnam County are mostly rural areas where unemployment and poverty rates are generally higher.

The state's only public technological university, Tennessee Tech University offers more than 200 undergraduate and graduate programs of study to about 10,100 students[4]. According to U.S. News & World Report, Tennessee Tech ranks in the top 150 Best Public National Universities, and Tennessee Tech graduates leave with the least debt of all public universities in Tennessee[5]. Tennessee Tech's College of Engineering receives one of the Best Undergraduate Engineering Programs rankings consistently. Tennessee Tech's Computer Science (CS) program[6] enrollment is increasing at a higher rate than any other departments in the college. There are 516 students in the current semester enrolled in the CS undergraduate and graduate programs. The combined CS student population is composed of 13.57% female students and 86.43% male students. In regards to ethnic background diversity, 15.31% are from underrepresented ethnic backgrounds.

In the computer science curriculum, there are three focus areas of studies: cybersecurity, data science and high-performance computing. The majority of the students (around 44%) are in the cybersecurity concentration and enrollment quadrupled in the four years since it started. We are the only program in Tennessee that offers student specialization in cybersecurity in CS at all three levels of education: bachelor's, master's and doctorate.

Tennessee, as a state, has become nationally recognized as an educational reform and workforce development state with multiple programs supporting the goals set forth by the governor's office[7]. Education specific programs focused on post-secondary education reform include:

- Drive to 55 Alliance[8]: An initiative to get 55% of Tennesseans equipped with a college degree or certificate by 2025
- Tennessee Reconnect: An effort to aid adult learners in entering or returning to higher education to gain new skills, advance in the workplace, and completing a degree or credential.
- Tennessee Promise: The first PK-14 program in the nation providing Tennessee high school graduates the opportunity to complete an associate's degree tuition free

Although cybersecurity is not central to Tennessee's Drive to 55 initiatives, it certainly can serve as a catalyst to accelerate cybersecurity efforts in the state. Therefore, this places Tennessee in a special position to become a national example in using these unique initiatives to extend cybersecurity educational opportunities to both traditional and non-traditional student pipelines. The Middle Tennessee market has established itself as the healthcare management and technology capital in the nation, as well as a manufacturing technologies capital in the southeastern region. Middle Tennessee has an urgent need for the development of a stronger cybersecurity workforce to protect these vital infrastructures.

## Describe the role the Cybersecurity Education Research and Outreach Center (CEROC) at Tennessee Tech in training the next generation of cybersecurity professionals and the federal and state programs that you and CEROC participate in.

The Cybersecurity Education, Research and Outreach Center (CEROC) at Tennessee Tech University, virtually established in October 2015 and physically established in January 2016, is a Center of Academic Excellence in Cyber Defense Education (CAE-CDE) accredited by the National Security Agency (NSA) and Department of Homeland Security (DHS)[9]. The center was established by the Department of Computer Science and the College of Engineering to integrate university-wide existing activities and initiatives in cybersecurity education, research and outreach, the emphasis of which makes it unique in the state.

The mission of CEROC is heavily influenced by the federal CAE-CDE program and CyberCorps SFS programs and stands:

> ***To advance and support cybersecurity workforce development following the pillars of education, research, and outreach in producing the next generation of cyber defenders and finding solutions to security and privacy problems in cyberspace.***

With the overarching goals of increasing the number of qualified students entering the fields of cybersecurity and contributing to the capacity of the cybersecurity workforce, the activities of the center are centered on the following objectives:

1. To increase public awareness of information assurance and cybersecurity;
2. To supply adequately trained students in cybersecurity workforce pipeline;
3. To enhance students' knowledge, skill, research aptitude, and service-learning motivation through a program that values fair participation in education, research, and outreach
4. To create additional pipelines of qualified cybersecurity professionals in industry and federal agencies from Tennessee (and the region);
5. To increase women and under-represented minority students' participation in cybersecurity;
6. To promote and disseminate cybersecurity educational and research artifacts and experience in the academic community; and
7. To share expertise with partners through collaborative initiatives in cybersecurity workforce development and research.

To achieve these goals and support our mission, CEROC supports students with:

1. Scholarship opportunities to Tennessee Tech students in Computer Science within the CyberSecurity Concentration that allows for the completion of a graduate degree in half the time of a traditional path;
2. Technical and professional development infrastructure and training to supplement formal education and prepare students for challenging careers in cybersecurity in all sectors;

3. Opportunities for field-related work experiences and research guided by mentors from Tennessee Tech, and center partners;
4. Opportunities to participate in professional development events such as competitions and conferences in the field;
5. Opportunities to participate in student communities and professional societies; and
6. Opportunities for active involvement in outreach and service learning at different events organized by Tennessee Tech.

At CEROC, we facilitate an integrated experience for our cybersecurity students ensuring their participation in informal education, research and outreach activities alongside their formal cybersecurity education as part of the CS curriculum. With the mantra of ***continuous learning, crowdsource learning and paying it forward***, our students are constantly challenged to immerse themselves into their educational experiences with the goals of enriching themselves and providing opportunities to enrich their peers and community around them. Here are words from one of our female students, S., who transferred from a Tennessee community college to our program:

***"With CEROC, I have learned in a short amount of time, that no matter my current skill set, I belong here and can achieve a positive impact on my community. This is due to CEROC making me realize that there is a bigger picture behind every little thing that I do, and therefore my sense of altruism has increased."***
She is currently an SFS scholar at Tennessee Tech and recently accepted a summer research internship offer from Oak Ridge National Laboratory (ORNL) for Summer 2020.

Tennessee Tech was awarded the **NSF CyberCorps SFS scholarship grant** in December 2015 (NSF Award 1565562). We were the first university in the State of Tennessee to be awarded the opportunity to manage this prestigious scholarship and remains the largest of such program in the state. The primary focus of the program was to produce candidates with M.S. degrees. With current extensions to the grant, we will produce approximately 32 workforce ready cybersecurity professionals over a span of five years. Twelve of them have graduated already with 10 serving in Federal agencies. Like D., *a minority student from Nashville, who came to Tennessee Tech uncertain about what he wanted to do after college. Through CEROC and the SFS program, he was able to recognize his passion for cybersecurity. He now works in the intelligence community and is using the knowledge and skills he gained through school to help defend the nation against foreign adversaries.*

Tennessee Tech is one of 10 universities that participated in the **CyberCorps 2Y Community College Pathways Program** working with three of our four community college partners in the state. Five community college students have joined during their sophomore year at their original school and transferred to Tennessee Tech for two additional years, allowing completion of a B.S. degree in three years.

One of them, A., *a transfer student from a Tennessee community college, received the SFS Scholarship while completing an associate's degree in computer science. It allowed him to quit his day job at a sports store and concentrate on his academic courses that he needed to transfer. It also allowed him to have the opportunity to go to a university to earn his bachelor's degree, which* *originally was not part of plan because of financial reasons. Being a recipient of the SFS Community College Pathway Program at Tennessee Tech is allowing him to acquire skills in computer science and cybersecurity to be ready for the future in cyber that he sees for himself now.*

The impact of the SFS program for our school is indisputably ground breaking. As a result of the center's CAE designation and the subsequent award of the CyberCorps SFS grant, the State of Tennessee, as part of the FY 2017 state budget process, appropriated "$500,000 to Tennessee Technological University to match funds provided by the National Science Foundation for cyber security research (year 1 of 4)", a total of $2,000,000 for the four-year period ending FY 2021. This non-recurring budget allocation was crucial in the establishment of CEROC and is the sole source of its logistical operations. The funds have been allocated each year in alignment with the center's three pillars of operation namely, education (20%), research (40%), and outreach (15%). CEROC has made every effort to maintain administrative overhead at approximately 20%. The funds provide for salaries for center staff, research infrastructure including the cyber range, mini-grants for faculty researchers, support for graduate and research assistants, and support for the many outreach activities that are conducted throughout the year for the community at large.

Tennessee Tech was awarded the **Department of Defense Cyber Scholarship (CySP)** grant in May 2018 (Award H98230-18-1-0315). This puts Tennessee Tech among an elite group of universities in the nation to have both the DoD CySP and CyberCorps SFS programs, not to mention the only university in the State of Tennessee to have such a distinction. The primary focus of the program is to produce candidates with M.S. degrees, and currently we have five CySP scholars (3 male and 2 females). One of them is Q. *came to Tennessee Tech with very minimal ideas about his future career plans because of limited exposure to STEM during prior years of schooling. After switching his major several times, he finally found his passion in computer science and, cybersecurity. Aftr becoming a recipient of the DoD CySP scholarship, he is be able to hone his skills in defensing against cyber threats to become a shovel-ready future employee of the intelligence community.*

Tennessee Tech received NSF Awards for two related projects: **CReST CyberWorkshops**: Resources and Strategies for Teaching Cybersecurity in Computer Science (Award# 1438861) and **SecKnitKit (Security Knitting Kit):** Integrating Security into Traditional Computer Science Courses (Award#: 1140864) through 2012 to 2017. These projects helped in creating a security mindset in computer science faculty and empowered them to include important security topics that may otherwise be unfamiliar. The faculty workshops we organized reached over 150 faculty from diverse institutions across the nation who committed to transform cybersecurity education and increase the number of undergraduate students recognizing the importance of security. These projects continue to provide computer science students at Tennessee Tech, and other institutions who adopted our curriculum, with the appropriate skill set to meet the national need for a cybersecurity workforce.

Other informal education and professional development activities that CEROC supports for our students to train them as the next generation of cybersecurity professionals are the following:

### Hands-on Skill Training

Hands-on active learning is an integral part of education. It has been found that students actively engaging with concepts from course material learn more effectively. For students to effectively contribute in the defense of our nation in cyberspace, it is crucial for them to gain experience in active hands-on offense/defense training. Most of the courses with security content already contain hands-on exercise modules for students to actively engage with course concepts. Additionally, CEROC supports and facilitates the following student skill training interest groups:

- The ***Capture the Flag (CTF) cyber interest group*** that meets to hone interest and gain active learning experiences in CTF style of activities. The group competes in a variety of online CTF competitions such as National Cyber League, Virginia Cyber Summit, picoCTF. An additional goal for this team is to facilitate local competitions and events for K12 CTF teams either at on-campus events or on-site at local schools.
- The ***Defensive cyber interest group*** cultivates interest and supports training in defensive skills. The primary competition for this team is the Collegiate Cyber Defense Competition. Other competitions that they participate in are the DOE CyberForce competition and Hivestorm.
- The ***Offensive cyber interest group*** (largest group among the three) meets to practice and acquire offensive proficiencies. The primary competition for this team is the Collegiate Penetration Testing Completion. Other competitions they participate in are DOE CyberForce, SFSCon etc.

Last year, CEROC hosted the Collegiate Penetration Testing Competition (CPTC) for the Central Region, welcoming 75 of region's best students in the offensive security domain of cybersecurity from 10 schools. CPTC provides a vehicle for up and coming cybersecurity student teams to build and hone the skills required to effectively discover, triage, and mitigate critical security vulnerabilities. We will host the competition again this year.

### DoD and NSF Funded Cyber (Eagles) Range

With funding form DoD and NSF, CEROC has developed the Cyber (Eagles) Range, which is a virtual infrastructure that supports our education, research and outreach activities. This space is supported by virtualization hardware located in the university's datacenter, which is also physically and logistically air-gapped through the wired and wireless network supported by Information Technology Services (ITS). The range is extensively used in various activities such as: special interest group training, competitions, cyber war games, lab support in courses such as IT Security, Reverse Engineering and Ethical Hacking, K12 lesson plans, outreach activities and research projects.

## Cybersecurity Student Club

Tennessee Tech CyberEagles[10] is a student organization with a mission to raise computer and information security consciousness and proficiency of students in using, designing, developing and operating computing technology. The club welcomes student members interested in cybersecurity from departments across the university. Currently there are 100+ members, and membership continues to grow. The club has been recognized as a National Cybersecurity Student Association (NCSA)[11] affiliated club. It is very active and conducts bi-weekly seminars for club members such as invited talks by external speakers from diverse walks of life including research, industry, and government service sectors, virtual CAE NSA Tech talks, training seminars., and regional security conference attendance. The club has been a very positive influence on our students. Aside from the educational benefit of these meetings, CyberEagles is an important part of our internal recruitment strategy to get more Tennessee Tech students to consider the cybersecurity focus area. Senior members of the club are strongly encouraged to take leadership roles to improve their organizational and management skills and provide mentorship to newcomers.

Tennessee Tech also founded the first installation of WiCyS student chapter, CyberEagle-W(omen)[12], which is now among a group of 89 in the nation. The 25+ members in the student organization under hosts a variety of professional development activities monthly to all students who are interested to attend. It includes networking events, technological activities, field trips and guest speaker engagements.

## Service Learning with Cyber Reviews

CEROC has collaborated with the Tennessee 3-Star Industrial Assessment Center (IAC) at Tennessee Tech to provide cybersecurity risk assessments for small to mid-sized manufacturing companies in the State of Tennessee. As part of a joint effort funded through a grant with the Department of Energy, CEROC and the 3-Star IAC deploy student assessment teams led by CEROC's assistant director to conduct cyber reviews for local and regional manufacturing companies and small businesses. The reviews involve an on-site evaluation component providing students the opportunity to exercise their team and client development skills. Once data collection activities (via survey and personal interview) are complete, the students begin processing the collected data and evaluating it against a scoring rubric based upon the NIST Cybersecurity Framework and other NIST SP documents. A final report is delivered by the student team with recommendations for improvement of their security posture. CEROC has also piloted a program of K-12 school district reviews with county districts. This program focuses on the unique challenges associated with school districts.

## OPM CyberCorps SFS New Scholar Bootcamp

Since 2016, Tennessee Tech has organized the annual Cybersecurity Scholar Bootcamp (funded through an extension of our original SFS grant) every summer. This first of its kind camp provides cybersecurity scholars from across the country an opportunity to attend a day and a half workshop covering a wide variety of essential soft skills for their future academic and professional careers. Topics covered during the camp include: financial planning, communications, diversity awareness, resume development, and research ethics and methodologies. The Tennessee Tech cohort have an additional half day of training conducted in the Volpe Library to become further acquainted with University research resources. Over the last four years, the bootcamp supported more than 175 new SFS scholars nationwide. CEROC also includes Tennessee Tech students participating in the DoD CySP program in this bootcamp given such a camp does not currently exist for the DoD program.

### Cybersecurity Ambassador Program

We encourage our scholars to participate in locally hosted events as project presenters, counselors, panel participants, and guest facilitators. This requires them to practice and exercise their soft skills for audiences in K12, higher education, and industry. These social settings are a key part of our holistic approach to scholar development. The students effectively serve as ambassadors of our program to the external community.

## Faculty-Mentored Research

### Research Engagement

With healthy Ph.D. production and financial commitment to research, in 2019 Tennessee Tech bolstered its position in the Carnegie Classification and moved up as a R2 university — a doctoral university with high research activity[13]. This is indicative of Tennessee Tech's increased performance in research/scholarship doctoral degrees and research expenditures.

In Computer Science, there are thirteen faculty who are active in security-related research and are working with students in cybersecurity-related research projects as mentors. In fact, the University recently hired five new Computer Science faculty to support our research mission. Research areas in security include (but not limited to): cyber physical systems security, internet of things (IoT) security, vehicular ad-hoc network security, network and 5G security, DarkNet, healthcare security, web application security, and machine learning assisted security. Students have multiple opportunities to conduct research under the guidance of CS faculty mentors through sponsored projects, courses in curriculum, thesis and project requirements.

### DOE Oak Ridge National Laboratory Collaboration

Our faculty and graduate students have been conducting research with the scientists and engineers at ORNL in various Department of Energy funded research projects. They have been working on the following funded research Projects: 1) Detection and Analysis of Malware in Critical Infrastructure, 2) Black Box: Highly Secure Environment for Health Data Computation, 3) From can't to CAN: Attack Prevention & In-situ Detection of Advanced Attacks on Controller Area Networks, and 4) Intrusion Detection Using Multimodal Machine Learning. Apart from these, there are several unfunded projects that our faculty and students are working on with ORNL. Many of our graduate and undergraduate students work in cybersecurity area research projects as interns in summer or regular semester at ORNL. ORNL scientists teaches cybersecurity-related classes at Tennessee Tech and supervise Ph.D. and Master's students. Tennessee Tech's Computer Science department has a special Ph.D. program for ORNL employees who do not have Ph.D. Our faculty also travel to ORNL to teach classes.

## NSA INSuRE Project Participation

We also participate in the INSuRE (Information Security Research and Education) project [14] which has been supported by NSA since 2012 for current and potential CAE-R institutions since 2012. The project cultivates research acumen, skills and experience for undergraduate and graduate students through a research network of 19 universities, multiple agencies and national labs. Students engage in interdisciplinary, distributed-teams to address information security problems of national interest. Our students have bene participating in INSuRE projects since 2018.

## Outreach Engagement

CEROC conducts multiple outreach projects for the K-12, higher education, and industry sectors. Our outreach programming especially provides opportunities for students in rural schools to be aware of cybersecurity careers and prospects, encouraging consideration of cybersecurity as a field of study, sparking interest in cybersecurity education and competitions, and encouraging participation of under-represented populations in STEM areas. Along with other Tennessee Tech students, SFS and Cybersecurity Scholars actively participates in various outreach activities hosted by CEROC, which includes but not limited to the following:

- Women in CyberSecurity conference
- Faculty development workshops (onsite and offsite)
- Computer security awareness and training workshop for Tennessee Tech staff
- Activities at the Tennessee Tech STEM Center for elementary and middle school students
- Cybersecurity discovery workshop for incoming students
- Cybersecurity reviews for manufacturing and small bushiness
- CyberPatriot support and mentorship in local schools
- Cyber Encounter workshop for high school teachers and students
- GenCyber summer camp for high school students, teachers and counselors
- GenCyber on Wheels with STEMmobile deployments to area schools

## NSA and NSF Funded GenCyber Program

Tennessee Tech has been awarded funds from NSA and NSF to conduct GenCyber camps since 2016. CEROC organizes a one-week camp focused on cybersecurity hands-on exercises with and without use of technology. CEROC camps have focused on high school students (rising 9th grade – rising 12th grade). Over the last four years, we have directly interacted with 510 students (155 in the state, and 355 students in four other states through GenCyber Day WiCyS events). Additionally, we have directly interacted with 12 teachers and 13 school counselors in the Middle and East Tennessee regions. These specific contacts have indirectly influenced thousands of students over the past three years.

Tennessee Tech has begun to see students from our GenCyber programs become freshmen in the Computer Science program and choose the cybersecurity concentration, like T. one of our camp participants. *A local high school student, he came to our GenCyber Camp in Summer 2017. The camp inspired him to pursue a career in cybersecurity, and he joined our program at Tennessee Tech with the hope to gain a better understanding of cybersecurity and computer science as a whole. He said,*
"***The camp was the deciding factor in choosing Tennessee Tech as my school and ultimately choosing cyber as a career.***"

## NSF Funded Cyber Encounter Project

Funded through an extension of our original SFS grant, this project seeks to empower high school teachers to bring extracurricular cybersecurity education to their students in high schools across the nation through a series of "Cyber Encounters." In close collaboration with the SANS Institute, the partners in the project include CSforAll, Computer Science Teachers Association (CSTA) and WiCyS. We are reaching around 150 teachers and 1,000 students across six states, Colorado, Indiana, New Jersey, Virginia, Tennessee and Texas, through workshops, instructional materials, pop-up cybersecurity challenges and the Girls-Go-CyberStart competition[15].

## NSF Funded WiCyS Project

The Women in Cybersecurity (WiCyS) project was launched in 2013 with support of a National Science Foundation grant (Award# 1303441). The annual conference brings together women (students/faculty/researchers/professionals) in cybersecurity from academia, research and industry for sharing of knowledge/experience, networking and mentoring. Every year Tennessee Tech brings around 20-30 students to volunteer and actively participate at the annual WiCyS conference. More about the initiative will be discussed later.

## Summary

At CEROC, we believe that for a scholars' professional development, exposure to education, research and outreach are all essential. While the importance of integration of education and research is clear, outreach in the form of service learning and civic engagement is an essential part of good scholarship and moreover, good citizenship. Research has shown that service-learning opportunities can increase students' interest in STEM disciplines. Service learning has also been found to increase students' knowledge. J., one of our SFS scholars spoke to the importance of an integrated experience in education, research and outreach as facilitated by our program at Tennessee Tech.
From him: "***As a former high school teacher from Nashville, my integrated experiences in education, research and outreach is preparing me to serve my community better as a cyber professional. The experience has strengthened my enthusiasm for education both in and out of the classroom by providing me with a community of like-minded individuals where I am able to learn and grow. I have also been able to participate in compelling research opportunities to potentially advance the field that I would otherwise not have access to and engage with diverse groups of people through outreach projects allowing me to be of service to others and make a significant impact.***"

## Address the strengths of these federal programs and the challenges that universities face in adopting them.

### Centers of Academic Excellence Program

Strengths

The NSA DHS CAE program[16] was the catalyst for the opportunities that would ultimately come available to our center. As a result of our Center of Academic Excellence – Cyber Defense Education (CAE-CDE)[9], CEROC became eligible for consideration for the CyberCorps SFS grant. The CAE recognition allowed us to become a virtual center, and later, CyberCorps SFS would make us a "bricks and mortar" unit. Our CAE designation also qualifies us to apply for scholarships such as the Department of Defense Cyber Scholarship Program and other educational and capacity building grants only available to CAE institutions. It allows us to be part of the over 300 member CAE community portal[17] and symposium that meets once a year. We also receive guidance from a CAE Seal - a federal government cyber professional and participate in the CAE Tech Talk program[18].

Challenges

The application and maintenance process for the current CAE program is a very laborious process. This is especially true of the current knowledge unit mapping process. Even small changes in curriculum can generate a significant remapping/reporting process. As mentioned earlier, CEROC will be participating in a pilot program and working group with nine other universities in a new designation process that will better align with existing program accreditation efforts such as ABET. We look forward to the process improvements that will come from this work.

### NSF CyberCorps SFS and DoD Cyber Scholarship Program (CySP)

Strengths of CyberCorps SFS and CySP

The CyberCorps Scholarship for Service program[19] began in 2001. As per the National Science Foundation, since the initiation of the program, 4,040 scholarships have been issued nationwide. To date, 3145 students have completed their academic work and 2,834 have entered government service in a cybersecurity role. The remaining 311 students are processing their clearances, searching for a position, have been released from their obligation, repaid their debt, or have been referred for collection. Of the 2,834 graduates, 2,123 (75%) have gone to a federal agency; 191 (7%) have entered state, local, or tribal government; and 520 (18%) have gone to Federally Funded Research and Development Centers (FFRDC).

The Department of Defense Information Assurance Scholarship Program began in 2001. This program was scheduled for shutdown in 2016 but was revived in 2017. It was renamed the Department of Defense Cyber Scholarship Program (CySP) in 2018. The program provides the Department of Defense exclusive access to a large pool of highly-qualified cybersecurity students to fill much needed cybersecurity roles required to defend our nation's interest. To date, 550 students have received scholarship funding through one of the two phases of the program. These students have attended one of 127 institutions across 40 states and Puerto Rico.

Both of these federal scholarship programs are very comparable. The differences are:

- SFS is awarded through NSF and DoD is managed by NSA.
- DoD is limited to only DoD agencies, while SFS is open to all Executive Branch agencies.
- DoD scholarship comes with a job offer, while an SFS scholar is responsible for finding a job.
- DoD agencies select the scholarship recipient, and the awardee university picks the SFS scholarship recipient.
- SFS scholarships are granted through multiple years, and DoD scholarships must be renewed every year.

The impact of both SFS and DoD CySP program is tremendous. The programs play a critical role in addressing the critical national demand, especially in federal agencies, for highly trained professionals in cybersecurity and provides a way for students to serve their country in a civilian role. The programs allow universities to continue to attract and retain the best and brightest in the nation to defend our country in cyberspace. It provides a paid opportunity for future cyber professionals to enter the market without a huge financial burden to follow them. Many of the recipients choose to remain in their agency roles after the job commitment is complete.

Many of the students who become SFS or DoD scholars would not have considered cyber careers otherwise. As an example, consider S., a top athlete and Summa Cum Laude female student with multiple opportunities ahead of her. However, she decided to pursue graduate school as a SFS scholar and writes:

***"CEROC and the SFS program has not only provided me with the means to attain a valuable and well-respected degree, but also provided me with a network of support, a group of like-minded and inspiring friends, and invaluable academic and financial resources. Without this program, I likely would have never aspired to have a career in cyber and certainly would have never considered applying for a federal position. Now, having done so, I have found a passion for public service and could not feel more excited for my career to come."***

Another relevant example J., *who is a second-generation college student from a rural Tennessee town with a population of less than 2,000. He was raised by a single mother who was a school teacher, and partly by his father, who worked an agricultural farm. He became an SFS Scholar in Spring 2019 and served his internship in the Department of Homeland Security in Summer 2019. Because of the SFS program, he is on his way to becoming a cyber professional and serving his nation.*

Challenges with SFS

CyberCorps SFS is a substantial program to manage for a university. While all grant programs have a given level of paperwork to process throughout the lifecycle of the grant, CyberCorps has the additional administrative load of managing and reporting the financial and professional portfolios of the student participants. In addition to tuition management, reimbursements must be managed for health insurance premiums, professional development expenses including travel management, and supplies expenses. Of particular challenge to CEROC early in our program, was the definition of which expenses aligned with each funding classification. CEROC ultimately helped to contribute best practices and clarification of policy to OPM in regards to how these funding classifications could be managed in schools.

The payback process for CyberCorps SFS is also a challenge for universities. Should a student leave the program prematurely or fails to gain employment with a federal agency as agreed in the scholarship contract, the student must return all of the funding that they have had received from the scholarship. Unlike the Department of Defense program that manages student paybacks at the program office level, CyberCorps SFS places the collections burden on the university loan accounting office. CEROC in conjunction with university administration has worked out a payback process as part of the university's student agreement. This process and form have been shared as a best practice with OPM.

Another unexpected challenge that we address is mental health issues, particularly depression. Students in high academic settings are not immune to stress and this may result in depression[20]. While there are means of dealing with depression, students may not be comfortable discussing the issue or seek counseling, fearing it will be viewed negatively in their SF-86 background check process. Mental health supports, without fear of SF-86 process harm, must be considered to help this group learn the appropriate mechanisms to deal with the stressful environments that they may encounter. This also promises to increase their longevity in the sector by avoiding the burnout that is becoming all too common among long-term cyber professionals[21].

Competition with industry will continue to be a challenge for federal scholarship for service programs. Private industry can pay much higher salaries than government will ever be able to consistently pay, outside one-time signing bonuses. The burden to the university in this matter is the introduction of enhanced vetting mechanisms by which candidates have to be evaluated for consideration. The university must seek individuals with a public service desire over a financial gain desire. This is increasingly difficult to address given private industry is ramping up their cyber operations at a rate similar if not faster than the federal government. CEROC spends a great deal of time with potential candidates to make sure that there is no "buyer's remorse" after entering the program.

### Challenges with CySP

In order to qualify for the DoD CySP program, an institution must be designated a Center of Academic Excellence (CAE) via the CAE Community process. This designation provides an assurance for reviewers that the degree granting program is providing appropriate instruction with appropriate frameworks for cybersecurity studies. CEROC completed this process in October 2015 and will be part of a pilot group which will undergo the new review process in 2021. This process is no small task and may be intimidating for some smaller institutions. The CAE Community is currently working to streamline the process (see pilot group reference above) and provide additional supports for institutions seeking this designation including mentoring programs.

The program does share some of the same administrative load mentioned in the CyberCorps SFS program. Most of the same student management activities are required for this group. For schools that are so blessed to have both programs, a full time employee is required to manage financial aspects of the two programs.

Another challenge of this program, as mentioned in the CyberCorps SFS review, is identifying students who are public service motivated rather than financially motivated. As mentioned earlier, government positions do not pay at the same level as a corresponding private industry. Given the DoD-focused nature of this program, there are fewer agencies participating, which may also not be as attractive to some students.

## NSA – NSF GenCyber Program

The GenCyber Program, funded by the NSF and NSA, provides funding to grant-awarded institutions to conduct summer cybersecurity camps for K-12 students. As stated on the program's webpage "The goals of the program are to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation, help all students understand correct and safe on-line behavior and how they can be good digital citizens, and improve teaching methods for delivery of cybersecurity content in K-12 curricula."[22][23]

### Strengths

Over the last six years, the camps have reached nearly 20,000 students and teachers nationwide. It plays a significant role in increasing awareness in cybersecurity and building the pipeline of cyber professionals. In our school, it has helped students in our state and region to consider cybersecurity as a career and create a pipeline of students to our cybersecurity program.

### Challenges

One significant challenge we face with GenCyber is the timeline of award announcement. Since it is typically awarded late April or early May, it becomes difficult to recruit students for a summer camp that is one to two months away, especially when Tennessee schools close for summer in mid-May. In several cases, parents and students have already made their summer plans which results in us losing some very viable participants.

In past years, we conducted combination camps for high school students, teachers and school counselors. Feedback from our camps showed that this has been very effective to bring these groups together with dedicated, focused sessions specifically for them. Since the new GenCyber directives do not allow combination camps, we are not able to continue with that approach. As our center is extremely busy, it is very difficult for us to conduct two separate camps. Another related problem is that we cannot offer dedicated camps for guidance counselors based on those same directives. We feel that is a missed opportunity. Since our inclusion of school counselors in the camps, being the only school to have ever included them, we have continued relationships with these counselors who often tell their students about cybersecurity careers. They will send students to visit us for further information, resources and opportunities. We have had multiple students join our program because of the school counselors' summer camp engagement.

## What are the challenges with diversity and inclusion in the cybersecurity workforce? What progress has been made? What can be done to improve these efforts?

The challenges in diversity and inclusion in the cybersecurity workforce is not new and has been the topic of conversation is many avenues and publications. Yet we are still at 20-24% on female representation and 26% on minorities in cyber workforce, according to 2019 (ISC)$^2$ Cybersecurity Workforce Study[24][25]. What we need to do now is to take on directed actions to address these challenges and share best practices in doing so. Here are the challenges, in short, for increasing diversity and inclusion before we discuss how our Women in CyberSecurity (WiCyS)[26] effort is addressing these challenges:

- Stereotypical notion
- Unconscious bias
- Lack of:
    - Awareness
    - Resources
    - Visibility of role models
    - Access to mentors
    - Social support
    - Inclusive actions/environment
    - Directed actions to hire diverse candidates
    - National/regional/local community
- Inadequate advancement and professional development opportunities

In 2012, we (Tennessee Tech University, University of Memphis and Jackson State Community College) had reached out to the National Science Foundation's SFS Capacity building program to seek funding to create a conference and community of women in cyber so that we could collectively address the challenges mentioned. The project was awarded in 2013 and our journey began (Award# 1303441). I am proud to let you know that over seven years (2014-2020) and with ~3.5 million dollars in industry sponsorship, WiCyS has:

- awarded ~ 3000 student scholarships
- awarded ~ 340 faculty scholarship
- approximately 6400 attendees over 7 years

Not only the flagship conference[27] for women in cyber, WiCyS has become, regardless of gender, the largest security conference in the nation with international reach that ensures comparable representation of students and professionals in the audience and comparable representation from academia and industry (public and private).

The need of community and sustainability of the initiative encouraged the creation of the WiCyS 501(c)(3) non-profit organization (unaffiliated with Tennessee Tech) in 2017 with a mission to build a strong, gender-diverse cybersecurity workforce by facilitating recruitment, retention and advancement for women in the field[28]. With the support from three foundational partners: Cisco, Facebook and the Palo Alto Networks and continued strategic partnership with seventeen organizations (Amazon Web Services, Bloomberg, Cisco, Lockheed Martin, Optum, Google, SANS Institute, Cyberbit, Equifax, PayPal, Target, Blue Cross/Blue Shield, Nike, HERE Technologies, IBM, Palo Alto Networks, and UC-San Diego), WiCyS offers the following initiatives to its community of more than 6,000 members (approximately 48% students and 52% professionals) to collectively take on the aforementioned challenges in gender diversity:

- Annual conference
- Student chapters: 89 chapters in 89 campuses across 35 states
- Professional affiliates: 15 affiliates across 20 states
- Speaker bureau featuring accomplished role models
- Job Board++ for yearlong engagement between opportunity seekers and providers
- Webinar series to promote and disseminate knowledge, experience and resources by female cyber professionals and role models
- Annual virtual career fair to bring job seekers virtually to industry
- Veteran Fellowship Award to enable female veterans to participate in WiCyS conference
- Veteran Apprentice Program to place female veterans in cyber careers (in progress)
- Industry Leadership Summit to bring together thought leaders to take action for certain challenges in cyber industry with diversity and inclusion
- Online member forums to allow exchange of ideas / thoughts / concerns / resources / opportunities among members
- Exclusive community for: mentors, veterans, ally, educators, chapters and affiliates

WiCyS has been successful because it is, in all true sense, a community, dedicated to work together in moving the needle in gender diversity. It is a community of

- like-minded peers who share knowledge and experiences
- mentors and mentees who thrives on their mutual relationships
- opportunity providers who make intentional efforts to seek out underrepresented talents
- resource providers who share with those in need
- role models who inspire others to excel

In 2013, women's representation in the sector was 11%. In 2019 the percentage has increased to 24%[29]. WiCyS alone cannot take credit for this increase in representation. There are other efforts in this area, such as EWF[30], The Diana Initiative[31], WISP[32], Women in CyberJutsu[33] – to name a few, that are also contributing in their own ways in different extents to the cause.

Underrepresentation in cybersecurity is not just a threat to diversity and inclusion but also a threat to workforce pipeline. If we are to attract more talents in cyber, we must reach out to the 50% of STEM talent pool that consists of underrepresented groups. As diversity fosters collaboration and creativity, today's complex challenges in cyber can be tackled better with diverse teams.

In regards to how government can help to improve efforts in increasing diversity, I have the following recommendations:

- Support and broaden funding for federal research and capacity building programs, such as NSF's CyberCorps SFS program that enables universities and community colleges to make tangible and significant steps towards gender balance in cyber and strengthens government's cybersecurity capacity. The WiCyS organization is a result of such investment.

- Support non-profit programs like WiCyS and others who continue to empower and support women in this field in effective ways by directing funding resulting from educational, workforce development, military and personnel programs and establishing long term support grants with success metrics aimed to show progress in improving gender balance in cybersecurity workplace.

- Establish federal legislation to encourage and provide incentives/resources for public and private sector organizations who:

    - Show intentional, directed efforts in creating bias-free and inclusive work cultures
    - Invest in alternative paths to get underrepresented groups in cyber, such as retraining to transition from low demand jobs to high demand cyber jobs, offering training and apprenticeship opportunities to allow stay at home mothers, veterans and their spouses to return or transition to cyber jobs.

- To close the gender and skill gap in cybersecurity, we must find ways to make a career in cybersecurity inviting for all. Society and the media often portray the dark side of the field. The public often hears about negative events like attacks and breaches from newspapers, television, and other media. We do not talk about how our experiences in today's technological world can only exist as per our expectation, because cybersecurity is at work behind the scenes. Parents and children are left in the dark about what cybersecurity really means besides attacks and hacks. Without understanding the impact of cybersecurity in our lives and society and awareness of the breadth of careers in cyber, from technical roles to non-technical ones, as well as the opportunities in cybersecurity, the younger generation cannot and will not consider careers in cyber.

## Discuss the challenges and opportunities to cybersecurity education at the K-12 level.

This generation of digital natives have been introduced to technology as the norm for communications, entertainment, and daily life logistics. High-speed Internet connections are considered a standard part of home, school, and business utility packages alongside services such as water and electricity. This connectivity fuels home activities, school activities and the cross-section of these two worlds where curriculum is delivered via online platforms. Homework may require a Chromebook rather than a notebook. This same connectivity fuels communication by email, SMS messaging, social media, and messaging within entertainment and gaming platforms.

Not only do our children expect access to connected devices within their home and school environments, they also expect to be connected wherever they go. A recent study by Common Sense Media has revealed that 53% of children own a smartphone by the age 11. This percentage increases to 69% by age 12.[34] These children are very comfortable with using technology and gaining information delivered by technology platforms. These children are ready for a new level of education, which should include computer science and cybersecurity at its core, not only to provide support for lagging the workforce pipeline for such jobs, but to support cyber safety for themselves and their families.

### Challenges

The challenges in cybersecurity in K-12 are significant from both an educational and operational standpoint. While K-12 districts have increased focus on other STEM subjects over the past decade, computer science and cybersecurity have not seen the same exponential growth of focus. Not until recent years have districts begun to develop their first computer science courses. Thirty-three states now have some sort of computer science curriculum initiatives underway [35]. This is a great milestone for cybersecurity since a majority of jobs in cyber requires a computer science education. More work is needed to have cybersecurity in K-12 reach this same level of success.

The greatest deterrent to cybersecurity intrusion is end user education. Despite the Universal Service Schools and Libraries Program (a.k.a. E-rate) mandate to provide such education, many K-12 districts still struggle to provide basic security awareness training to faculty, students, and staff. This deficiency contributes to the effectiveness of phishing attacks that can lead to ransomware and other malware exploitations.

Strained IT budgets create challenges at multiple levels. First, most districts have limited personnel to address all IT issues within the organization. Generally, basic deployment and core system management must take priority allowing cybersecurity concerns to become secondary matters. Existing IT personnel may also feel unqualified to deal with advanced cybersecurity concerns and may delegate such issues to their E-rate-funded Internet Service Provider. Unless obtained through premium contracts, this support will be little more than some well-crafted firewall rules. Additional cybersecurity training opportunities are needed for K-12 IT professionals to address evolving cyber threats.

Secondly, most local IT budgets do not adequately cover cybersecurity hardware and software needs at a level that can mitigate ever-evolving cyber threats. E-rate, via Category 2 funds, only cover basic firewall support and fails to address more needs that are sophisticated. Some are calling on the FCC to provide additional E-rate funds to address these issues.[36] Such upgrades are especially important with the proliferation of technological devices supporting classroom activities.

Thirdly, K-12 IT departments may be fearful of providing support for cybersecurity education programs that require hands-on activities. With a lack of adequate infrastructure to address basic operations, organizations may be fearful to allow students to conduct the advanced activities required by cybersecurity training requirements for fear of advanced insider threats to core infrastructure. Some additional hardware and software supports are needed to provide a "safe lab" for such activities, and more internal expertise is required to maintain them.

Another challenge facing K-12 cybersecurity programs is educator staffing. Districts have been looking for additional STEM educators for years[37]. However, even among this limited population, it has been difficult to identify and recruit individuals to teach computer science and cybersecurity. Among the many reasons offered, educators primarily state a lack of training that prevents them from teaching these subjects. While more training is needed, imposter syndrome also affects the number of available educators who have more qualifications than they think.

## Opportunities

K-12 is very rich with untapped opportunities for addressing pipeline challenges within the cybersecurity spectrum. Instead of treating cybersecurity as a silo and introduce a completely new curriculum path, cybersecurity should be integrated with computer science education. In fact, many of the concepts in cyber could be delivered in such a way that would complement existing curriculum standards in language arts, mathematics, science and social sciences. This would allow for a comprehensive education experience that delivers the building blocks for computer science principles and AP computer science courses.

Several initiatives have been introduced to assist K-12 in the integration of computer science and cybersecurity into their curriculum. The United State Department of Homeland Security (DHS) Cybersecurity Education Training Assistance Program (CETAP) provides curricula and education tools.[38] Additionally, National Integrated Cyber Education Research Center (NICERC)[39] provides a wealth of curriculum resources covering STEM, cybersecurity, and computer science. Organizations such as CSforAll [40] have several programs with the express goal of advancing computer science education to all students.

A number after school programs now provide extracurricular opportunities for students to learn more about computer science and cybersecurity while providing a sport-like element to the learning experience. Consider the Air Force Association's Cyber Patriot program[41] which provides students the opportunity to compete at multiple levels and gain hands-on experience in cybersecurity. Another popular cybersecurity competition that takes place during both spring and fall semesters is the National Cyber League[42]. In addition to the cybersecurity skill development opportunities for both high schools and college students, this competition also provides participants scouting reports that can be used to complement resumes and college applications.

Another opportunity for student development, which also benefits the cyber operations of K-12 school districts, is student cyber internships. Most districts have a shortage of trained professionals to address basic IT infrastructure needs, let alone cyber threats to their digital infrastructure. Additionally, districts may face internal cyber threats from the very student population that they seek to protect[43]. It will be tremendous boost for school IT administrations if they can make use of that cyber talent in the form of cyber internships where positive educational and operational outcomes may be realized. If they lack the resources, schools should reach out to local higher education institutions to request support/mentorship for such cyber trainees.

## Address where Congress should focus future efforts to bolster the cybersecurity workforce pipeline.

Following are my personal recommendations to Congress based on my experiences as an educator who strives to make a difference in cybersecurity education and workforce.

### Funding and resources to NSF CyberCorps and DoD CySP program

The impact of the federal scholarship programs (SFS and DoD CySP) is undeniable. For students it is life changing; for the workforce it is a great return-on-investment (ROI); for the universities that receive such awards, it is transformational. Congress should consider more funding to these programs such that more students can eventually join national cyber workforce in the imminent future when cyberwarfare will become the weapon of choice. With more universities joining the elite list of scholarship providers, they can acquire more resources to manage these programs and build their capacities. As more universities build up their capacity, their impact on community increases in many folds.

### Revisiting the 80/20 rule in SFS students job placements

By legislation, 80% of the participants from the CyberCorps SFS program must work directly for the federal government. Select FFRDCs have been allowed to participate in the program in the 20% portion. These FFRDCs have budget to provide competitive salary compared to their federal agency counterparts. This heavy recruitment has now begun to put pressure on that 20% rule. Additionally, many national labs are offering positions that are contractor-sourced rather than a federal billet. Most jobs at these facilities are contractor-based given they are managed by Battelle. These positions now come under the scrutiny of the 20% rule. Either the policy is revisited or the law amended to address this issue in order to avoid an interruption of flow of qualified CyberCorps students to cyber positions in our national laboratories, who are crucial to protect nation's crucial infrastructure. This 20% rule also accounts for students entering state cyber positions and higher education.

### Allowing more SFS students to join public universities as educators

CyberCorps SFS program can make yet another positive impact on the cybersecurity workforce pipeline if Congress allocates a quota of SFS students to pursue doctoral studies and join the cybersecurity workforce as educators in higher education for public universities as their scholarship obligation. In the Taulbee Survey conducted by the Computer Research Association, evidence is shown that most Ph.D. graduates are following the model of many of their undergraduate peers and entering industry rather than academia or government. In 2014, 83 new cybersecurity Ph.D.s entered the workforce. Out of that 83, only 4 (5%) pursued tenure track faculty careers. In 2018, 114 new cybersecurity Ph.D.s entered the workforce with only 14 (12.2%) entering tenure track faculty careers. Cybersecurity faculty members are vital to educating cybersecurity professionals in undergraduate and graduate programs. When 62.6% of an already small pool of Ph.Ds. go to non-academic roles (2018 study), it drastically hampers the pipeline development of cybersecurity talent and the cyberspace defense goals of the nation.

## Allowing more SFS students to join State government workforce

Currently, only 20% of students can join non-federal agencies, like states and FFRDCs. And as mentioned before, FFRDCs obviously attract more students with higher salaries than any federal and state agencies can offer. This situation is very problematic for state cybersecurity workforce development.

In 2019, according to a report from crn.com[44], around 948 government agencies, educational establishments and health-care providers got hit with a barrage of ransomware attacks at a potential cost in excess of $7.5 billion. Most of these agencies were city and county offices. At least $176 million dollar was paid by multinational manufacturers and U.S. city and county governments for ransomware-related attacks. These types of attacks have increased 365% in the past 12 months. Attacked cities include (but are not limited to) Baltimore, Lake City, Jackson County, and Pensacola. Already, during the first few weeks of 2020, several ransomware attacks targeted county libraries, community schools, and medical centers[45].

Therefore, it is extremely crucial for state governments to be able to tap into the pool of talented SFS students so that they can get the needed help to secure their local infrastructures. Cyberspace does not have boundaries. A weak cyber infrastructure at the state level can serve as the weaker link that allows greater attacks on critical resources of the nation. Also, allowing talented students to join local and state agencies also incentivizes those who have obligations at home that restrain them to serve in the federal government through local efforts. This will also allow more underrepresented female students to enter the SFS program. Although currently the SFS program does not prohibit students to join state agencies, the 80-20 rule certainly restricts such choices. Maybe Congress can allocate a certain quota specific to the state agency placement of SFS students. As our states become stronger in cyber space protection, it will only strengthen the federal mission.

## Enabling innovative programs to include community college students in SFS and DoD programs:

The current trend and need for a qualified cybersecurity workforce demonstrate that for an entry level cybersecurity specialist, the requested education (based on online job postings) for bachelor's and higher degrees is 78% as compared to 21% for sub-BA level, with an average salary of $92,000[46]. It has also been noted that after an associate's degree, community college students can move to an entry level cyber security position having an average salary between $40-60K[47][48], with very limited scope of career progress. As reported[49], the number of jobs in cyber security based on the job postings with associate's degree were 3,033, as compared to 82,773 postings seeking bachelor's degree. At present, the total cybersecurity job openings across the U.S. are around 500,000[49] and within the state of Tennessee this number is around 5,600 with the cybersecurity supply demand ratio at 2.1. This growing gap cannot be fulfilled with graduates with associate's degree, and a pipeline of students needs to be created to motivate them to earn cybersecurity-focused computer science bachelor's degrees with the required skillsets to fill the workforce need.

To increase both the pipeline and diversity in cybersecurity workforce, we must find effective ways to include the diverse body of students in community colleges. Community college student bodies are more diverse than traditional 4-year programs. According to American Association of Community Colleges' January 2020 report, 56% of community college students are women and 25% are underrepresented minorities. Also, 29% of them are first generation college students or non-traditional students who entered community college after military service (5%) or blue-collar jobs or who leave due to home/medial situations.

More students and diverse students (first generation, working adults, veterans, underrepresented and minorities) will be able to find themselves in cyber careers of their choice leading to a broadening pipeline and diversity in cybersecurity workforce, if Congress supports programs that

- Educate community college students about cyber career choices (jobs requiring associate's technical cyber degree vs jobs requiring at least bachelor's degree)
- Enable them to succeed in either path (2-year vs 4-year cyber degree),
- Offer working partnership between 2-year and 4-year institutions for seamless transition of community college students from associate's degree to bachelor's degree
- Offer innovative ways to make community college affordable (e.g., tuition assistance) and/or accessible (e.g., online classes) for working adults and veterans to pursue their education

In addition, both public and private sector including federal agencies must rethink and reinvest how they can create more of entry level cyber jobs to offer to students with associate's degrees in cyber. As mentioned before, there is a scarcity of jobs that only require associate's degrees in cyber and majority of jobs in cyber require bachelor's degree. OPM program and SFS PI experiences also confirm that for students who go through SFS program and obtain associate's degrees in cyber, it is often difficult for them to find a job for which they can apply.

## Supporting programs enabling non-traditional pathways into cyber

To fill the workforce demand in cyber, it will be extremely unwise to solely rely on graduates from traditional pathways coming through academic institutions to fulfill all the jobs in cyber. There is a vast pool of workers that has the potential to be recruited and trained to join the cyber workforce. This group includes veterans and their spouses, workers in low demand jobs, and workers returning to work after family obligations. There are federal programs that already exist that support non-traditional pathway workers such as those offered by the Department of Labor, Department of Veteran Affairs, Department of Homeland Security, and Department of Defense, to name a few. However, more needs to be done to establish effective partnerships between these agencies and community-based educational or non-profit programs that can access a greater population utilizing their own programming.

Congress should support such educational or non-profit programs that enable populations of non-traditional workers to find careers in cyber through resources or training or apprenticeships opportunities or combinations thereof.

## Allowing to educate school counselors through GenCyber programs

There is an opportunity to provide cybersecurity workforce awareness training for school counselors at the middle school and high school levels so they are prepared to provide needed information to students who may not have considered the computing sciences as an area of study. Most K-12 counselors do not have knowledge of cybersecurity opportunities for their students and likely to assume a very technical view of cybersecurity rather than understanding the existence of many areas of cyber ranging from policy, governance, forensics, and technical. We need to help K-12 school counselors to become aware of the possibilities in cyber so that they can then educate their students. CEROC has had a great deal of success in this space by providing this training in two different GenCyber camps. In each case, new students were introduced into the program as a result of efforts made by these newly educated counselors. Special focus must be given to middle school counselors as the majority of their student populations have not made final career decisions.

## Supporting social campaigns to change image of cyber

To address diversity and inclusion (and pipeline, as a result), the limited view of cybersecurity and its stereotypical image must change in society. The public needs to understand the societal impact cybersecurity has in our modern day lives. Congress should invest in programs or campaigns that can take on the image problem of cybersecurity so that the public gets the message that cybersecurity is more than hacks, and its impact in modern society is undeniable. Only then, will it be received widely and more bodies, regardless of gender, color, and/or affiliation, will feel motivated to join the campaign to keep peace in cyberspace.

## Conclusion

Tennessee Tech earned reputation statewide for undergraduate engineering education and by far, offers the best overall cybersecurity education program in the state. Through CEROC's programs Tennessee Tech has developed a recognized brand in cybersecurity at the state and at national level in the education, government, and industry sectors. This has been possible only because of the support, opportunities and resources that we have received through competitive federal programs. Without such programs in place, CEROC might not have existed at its capacity today, and the wide impact of CEROC would not have happened. Federal programs such as NSA DHS CAE, NSF SFS, DoD CySP, DoD GenCyber are crucial to enable smaller schools like us to have bigger impact in their community, their region and the nation. We sincerely hope that Congress will continue to bolster its support for these highly effective federal programs and commission more of such programs that can empower more institutions like ours to contribute in the nation's cyber agenda in its own ways, with its own strengths and in its own community.

As we continue to do our part in developing the future cybersecurity workforce, I would like to end with a quote from one of our many students, who are hardworking, humble and optimistic about their future and their country. M. writes: "This program has given me the dream for something bigger in this life. It has given me the courage to keep going, to continue seeking knowledge, and to make a difference in the world."

It is my everyday privilege to work with a group of dedicated colleagues, staff and administration at the Center, the Computer Science department, the College of Engineering and the University who are committed to make an impact on students' lives and help them to fulfil their dreams. I sincerely appreciate the opportunity to provide input. I hope that Tennessee Tech, CEROC and I can continue to be a resource to Congress on this subject matter.

## Bibliography

[1] "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021." [Online]. Available: https://cybersecurityventures.com/jobs/. [Accessed: 08-Feb-2020].

[2] "Cybersecurity Supply And Demand Heat Map." [Online]. Available: https://www.cyberseek.org/heatmap.html. [Accessed: 08-Feb-2020].

[3] "About Tennessee Tech University." [Online]. Available: https://www.tntech.edu/about/. [Accessed: 08-Feb-2020].

[4] "Admission: Tennessee Tech University." [Online]. Available: https://www.tntech.edu/admissions/index.php. [Accessed: 08-Feb-2020].

[5] "Tennessee Tech Rankings." [Online]. Available: https://www.tntech.edu/about/rankings.php. [Accessed: 08-Feb-2020].

[6] "College of Engineering - Computer Science." [Online]. Available: https://www.tntech.edu/engineering/programs/csc/. [Accessed: 08-Feb-2020].

[7] "Publications and Maps - Tennessee Department of Economic and Community Development." [Online]. Available: https://tnecd.com/research-and-data/publications/. [Accessed: 08-Feb-2020].

[8] "Drive to 55." [Online]. Available: https://preprod.tn.gov/thec/learn-about/drive-to-55.html. [Accessed: 08-Feb-2020].

[9] "What is a CAE? | CAE in Cybersecurity Community." [Online]. Available: https://www.caecommunity.org/content/what-is-a-cae. [Accessed: 07-Feb-2020].

[10] "Cyber Eagles – Tennessee Tech University Cyber Security Club." [Online]. Available: http://blogs.cae.tntech.edu/cybereagles/. [Accessed: 08-Feb-2020].

[11] "National Cybersecurity Student Association." [Online]. Available: https://www.cyberstudents.org/. [Accessed: 08-Feb-2020].

[12] "Wicys - Tennessee Tech Student Chapter - Home | Facebook." [Online]. Available: https://www.facebook.com/ttuwicys/. [Accessed: 08-Feb-2020].

[13] "Tech bolsters Carnegie Classification." [Online]. Available: https://www.tntech.edu/news/releases/18-19/tech-bolsters-carnegie-classification.php. [Accessed: 08-Feb-2020].

[14] "Information Security Research and Education." [Online]. Available: https://insurehub.org/. [Accessed: 07-Feb-2020].

[15] "CyberStart High School Cyber Security Challenges and Games | SANS Institute." [Online]. Available: https://www.sans.org/CyberStartUS. [Accessed: 08-Feb-2020].

[16] "NIETP." [Online]. Available: https://www.iad.gov/NIETP/index.cfm. [Accessed: 08-Feb-2020].

[17] "A Hub for National Centers of Academic Excellence | CAE in Cybersecurity Community." [Online]. Available: https://www.caecommunity.org/. [Accessed: 08-Feb-2020].

[18] "CAE Tech Talk." [Online]. Available: https://capitol.instructure.com/courses/510/external_tools/66. [Accessed: 02-Oct-2018].

[19] "CyberCorps®: Scholarship for Service." [Online]. Available: https://www.sfs.opm.gov/. [Accessed: 08-Feb-2020].

[20] "Depression, anxiety rising among U.S. college students - Reuters." [Online]. Available:

https://www.reuters.com/article/us-health-mental-undergrads/depression-anxiety-rising-among-us-college-students-idUSKCN1VJ25Z. [Accessed: 07-Feb-2020].

[21] O. Ogbanufe and J. Spears, "Ogbanufe and Spears Burnout in Cybersecurity Professionals Burnout in Cybersecurity Professionals," 2019.

[22] "About GenCyber." [Online]. Available: https://www.gen-cyber.com/about/. [Accessed: 07-Feb-2020].

[23] CEROC, "Gen-Cyber Camps -:|:- Tennessee Tech." [Online]. Available: https://www.tntech.edu/ceroc/outreach/gen-cyber. [Accessed: 28-Sep-2018].

[24] "Strategies for Building and Growing Strong Cybersecurity Teams."

[25] "Women Represent 20 Percent Of The Global Cybersecurity Workforce In 2019," *Cybercrime Magazine*, 2019. [Online]. Available: https://cybersecurityventures.com/women-in-cybersecurity/. [Accessed: 08-Feb-2020].

[26] "Women in Cybersecurity Organization." [Online]. Available: https://www.wicys.org. [Accessed: 02-Aug-2020].

[27] "Women in Cybersecurity Conference." [Online]. Available: https://www.wicys.org/conference. [Accessed: 02-Aug-2020].

[28] "About the Women in Cybersecurity Organization." .

[29] "Women Represent 24 Percent of Cybersecurity Workforce, (ISC)$^2$ Reports | 2019-04-02 | Security Magazine." [Online]. Available: https://www.securitymagazine.com/articles/90071-women-represent-24-percent-of-cybersecurity-workforce-isc-reports. [Accessed: 08-Feb-2020].

[30] "Executive Women's Forum." [Online]. Available: https://www.ewf-usa.com/. [Accessed: 08-Feb-2020].

[31] "The Diana Initiative." [Online]. Available: https://www.dianainitiative.org/. [Accessed: 08-Feb-2020].

[32] "Women in Security and Privacy." [Online]. Available: https://www.wisporg.com/. [Accessed: 08-Feb-2020].

[33] "Women's Society of Cyberjutsu." [Online]. Available: https://womenscyberjutsu.org/. [Accessed: 08-Feb-2020].

[34] M. B. Robb, W. Hearst, and C. Newmark Philanthropies, "CREDITS Eva and Bill Price THE COMMON SENSE CENSUS: MEDIA USE BY TWEENS AND TEENS 2019."

[35] "33 States Expand Access to K-12 Computer Science Education in 2019." [Online]. Available: https://medium.com/@codeorg/32-states-expand-access-to-k-12-computer-science-education-in-2019-7d2357fe6f3d. [Accessed: 05-Feb-2020].

[36] "Should the FCC expand E-rate coverage to include cybersecurity? | Education Dive." [Online]. Available: https://www.educationdive.com/news/should-the-fcc-expand-e-rate-coverage-to-include-cybersecurity/562361/. [Accessed: 05-Feb-2020].

[37] "Lack of STEM teachers means fewer graduates for critical roles | Education Dive." [Online]. Available: https://www.educationdive.com/news/lack-of-stem-teachers-means-fewer-graduates-for-critical-roles/556110/. [Accessed: 06-Feb-2020].

[38] "Cybersecurity in the Classroom | National Initiative for Cybersecurity Careers and Studies." [Online]. Available: https://niccs.us-cert.gov/formal-education/integrating-cybersecurity-classroom. [Accessed: 05-Feb-2020].

[39] "STEM Curriculum, Cyber Curriculum, Cyber Security Curriculum, Computer Science Curriculum." [Online]. Available: https://nicerc.org/. [Accessed: 02-Oct-2018].

[40] "CSforALL Projects and Programs | CSforALL." [Online]. Available: https://www.csforall.org/projects_and_programs/. [Accessed: 06-Feb-2020].

[41] A. F. Association, "AFA CyberPatriot Website." [Online]. Available: https://www.uscyberpatriot.org/. [Accessed: 05-Feb-2020].

[42] "NCL | National Cyber League | Ethical Hacking and Cyber Security." [Online]. Available: https://www.nationalcyberleague.org/. [Accessed: 05-Feb-2020].

[43] L. Columbus, "It's Time To Solve K-12's Cybersecurity Crisis." [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2019/10/01/its-time-to-solve-k-12s-cybersecurity-crisis/#c1fdf14262b1. [Accessed: 05-Feb-2020].

[44] M. Novinson, "The 10 Biggest Ransomware Attacks of 2019," 2019. [Online]. Available: https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019. [Accessed: 08-Feb-2020].

[45] D. Kobialka, "Unhappy New Year: Ransomware Attacks Hit Schools, Hospital, California City - MSSP Alert," *MSSP Alert*, 2020. [Online]. Available: https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/malware-hits-schools-hospitals/. [Accessed: 08-Feb-2020].

[46] "Cybersecurity Career Pathway." [Online]. Available: https://www.cyberseek.org/pathway.html. [Accessed: 08-Feb-2020].

[47] "Associate of Applied Science (AAS), Cybersecurity Salary | PayScale." [Online]. Available: https://www.payscale.com/research/US/Degree=Associate_of_Applied_Science_(AAS)%2C_Cybersecurity/Salary. [Accessed: 08-Feb-2020].

[48] "Entry Level Cyber Security Annual Salary ($74,324 Avg | Feb 2020) - ZipRecruiter." [Online]. Available: https://www.ziprecruiter.com/Salaries/Entry-Level-Cyber-Security-Salary. [Accessed: 08-Feb-2020].

[49] "9 Reasons Why You Should Study Cyber Security Now | Rekeb.com." [Online]. Available: https://rekeb.com/why-you-should-study-cybersecurity/. [Accessed: 08-Feb-2020].

CEROC
CYBERSECURITY EDUCATION, RESEARCH AND OUTREACH CENTER

# Dr. Ambareen Siraj Biography

Dr. Ambareen Siraj is a professor of Computer Science and the founding director of Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC). She has served as the leader on several NSF and NSA education and workforce development grants. Siraj is also the founder of the Women in CyberSecurity (WiCyS) organization, an initiative to recruit, retain and advance women in cybersecurity. Her efforts to educate students and enhance the cybersecurity field of study goes beyond classes, research, outreach projects, workshops and conferences.

Dr. Siraj's research focus is on security in cyber-physical systems, Internet of Things, situation assessment in network security, security education and workforce development. She has authored or co-authored more than 50 publications.

She is a frequent speaker in various cybersecurity conferences on topics ranging from education, curriculum, workforce development, outreach, security issues & solutions for cyber-physical systems to diversity and inclusion in cybersecurity. Dr. Siraj is recipient of the -Colloquium for Information Systems Security Education Exceptional Leadership in Education Award in 2018.

## TESTIMONY OF MR. JOSEPH SAWASKY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, MERIT NETWORK, INC.

Mr. SAWASKY. Honorable Chairwoman Stevens, Ranking Member Baird, and Members of the Subcommittee, thank you for the invitation to present Michigan perspectives on the critical issue of cybersecurity workforce development. My organization, Merit Network, provides advanced networking, security, and community solutions to higher ed, K–12, libraries, and other nonprofits in Michigan. Given our mission-critical work across the State, we see firsthand the ever-increasing importance of cybersecurity and the desperate need to expand that workforce.

Our country faces threats constantly from adversarial organizations but quietly and diligently on the frontlines are our Nation's thin ranks of dedicated cybersecurity professionals. According to estimates, the United States has a shortfall of over a half million security professionals. In Michigan alone we have nearly 9,000 vacant positions now. These gaps are projected to widen.

Over the last several years, Michigan has developed a unique approach to developing a cybersecurity training ecosystem and a powerful tech platform for practicing skills. The Michigan Cyber Range was created through collaboration between the State, industry, and Merit beginning in 2012. The Cyber Range is one of the Nation's largest unclassified practicum environments for security professionals to test their skills in cyber defense.

The Range features a simulated city called Alphaville that contains a virtual city hall, school, library, and factory, among other things. In our game of five practice environments, Merit has engaged nearly 4,000 participants from Michigan and other States and even other countries in cyber exercises.

Additionally, with the support of the Michigan Economic Development Corporation, we've cultivated a statewide ecosystem of training partners called Cyber Range Hubs helping them train and certify students in a variety of cybersecurity courses using the Cyber Range platform in its course curriculum. This program represents a novel augmentation of traditional higher ed and K–12 courses in the State.

There are real challenges faced by our partner organizations in the education, government, and nonprofit sectors in recruiting a skilled cybersecurity workforce. The primary challenge facing nonprofits is an extremely low supply of available talent. This low supply results in high demand for employees, higher market salaries, and longer-than-average times to fill vacancies. Yet nonprofits support a vast array of essential societal services and are still charged with protecting enormous amounts of confidential data. They face the very same cyber threats as other sectors, but their ability to attract cyber talent is constrained. Compounding this problem, finding qualified teachers and trainers for cybersecurity courses is really difficult, exacerbating the situation for nonprofits in the industry overall.

There's consensus in Michigan that K–12 is the first key to improving the security talent pipeline. That pipeline starts in K–12, and it's essential that skill development and awareness of cybersecurity career opportunities begin at early ages. Given that this field is fairly new and rapidly evolving, there has not been a pervasive focus on it for K–12 students or teachers. It's imperative that we demystify and de-nerdify cyber career opportunities to broaden the appeal of this career path.

Additionally, we should expand student interest by providing more opportunities for underrepresented groups, including females and minorities whose participation in the cyber workforce has been historically low.

To help promote K–12 enthusiasm in cyber, Merit runs the Governor's High School Cyber Challenge. Last year, we had over 600 students and over 200 high school teams participate with the top 10 teams being invited to the final contest at the Governor's Cyber Summit in Detroit and the top three teams being awarded trophies personally by the Governor herself. Through this exciting event, Michigan has celebrated K–12 cyber talent in every corner of our great State.

Considering all this, State and Federal Governments have a critical role to play in bolstering the cybersecurity workforce pipeline. One, they should increase support to programs aimed at improving K–12 awareness and skill development for both students and teachers. Two, they should increase support for education, training, and certification, including early credentialing in both high school and college. Three, they should increase support for skill development for underrepresented groups to grow that pool. And, four, they should incentivize coordinated efforts between academia, industry, and government.

And to wrap up, I'd like to say that many organizations are only one cybersecurity position away from a major disaster, and it's essential that we all work together to develop and grow this now-critical part of the U.S. workforce. Thank you for the opportunity to provide Michigan perspectives.

[The prepared statement of Mr. Sawasky follows:]

merit
NETWORK. SECURITY. COMMUNITY.

*Merit Network, Inc.*
*880 Technology Drive, Suite B*
*Ann Arbor, Michigan 48108*

**Subcommittee on Research and Technology**
**Committee on Science, Space, and Technology**
**U.S. House of Representatives**
**Hearing on "*More Hires, Fewer Hacks: Developing the U.S. Cybersecurity Workforce*"**
**Merit Network Testimony**
**Joseph Sawasky, President & CEO, Merit Network**
**February 11, 2020**

## Introduction

First, I'd like to thank the House Subcommittee and its members for the kind invitation and opportunity to present Michigan perspectives on the critical issue of cyber security workforce development. Our country faces real challenges many millions of times every single day from adversarial organizations, including hostile nation states and criminal enterprises. When defenses fail for U.S. organizations, companies, governmental entities, educational organizations, healthcare systems, manufacturers and others experience major negative impacts to operations - affecting services to citizens and customers.

Quietly and diligently, on the front lines, are our nation's thin ranks of expert and dedicated cyber security professionals. However, according to the National Initiative for Cybersecurity Education (NICE), the U.S. had a shortfall of over a half-million cyber security professionals as of January 2019. According to NICE, in my home state of Michigan, we have over 9,000 vacant cyber security positions now. Estimates of the global cyber security workforce shortage has ranged from 1.5 million to 3 million unfilled positions, with a higher than average annual growth rate in demand for talent.

Cyber represents the next horizon of warfare and crime, and it is essential that our nation nurture, support and grow the pipeline of cyber talent for our country - from K-12 to higher education and through continuing professional development.

## Can you describe Merit Network's cybersecurity training programs, such as the Michigan Cyber Range?

The Michigan Cyber Range was created through a collaboration between the State of Michigan, industry, academia and Merit Network beginning in 2012 under then Governor Rick Snyder's administration. It is one of the nation's largest unclassified cloud-based practicum environments for current and aspiring cyber security professionals to test their skills at cyber defense and offense. The Cyber Range features a simulated city called Alphaville, that contains a virtual city hall, school, library, hospital and manufacturing facility, among other simulated servers, systems and networks. In this practice environment, Merit has engaged nearly 4,000 participants from Michigan and other states and countries in cyber exercises and training. Participants span the spectrum of organizations, representing industry, government, national guard, academia, and healthcare, among others.

Additionally, with the support of the Michigan Economic Development Corporation, Merit has cultivated a statewide ecosystem of training partners, called Cyber Range Hubs, from higher education and K-12, helping them enroll, train and certify students in a variety of cyber security courses using the Michigan Cyber Range platform and its course curriculum.

Beyond the unique Cyber Range collaboration, many Michigan colleges and universities offer traditional degree programs in information assurance, information security and network investigation. These degrees are typically offered within computer science or business information systems programs at two year, four year and graduate levels.

**What are the challenges faced by some of your partnering organizations, such as universities, state agencies and nonprofits, in recruiting a skilled cybersecurity workforce?**

The primary challenge facing partner organizations is an extremely low supply of available talent. According to NICE, the supply/demand ratio for all jobs in the U.S. is 4.9, but for cyber security positions, that ratio is only 1.9. This low supply results in high demand for employees, higher market salaries and longer-than-average times to fill vacancies. Non-profits have difficulty competing with for-profit organizations for talent, yet they are still charged with protecting enormous amounts of confidential information, advanced research, intellectual property, health information and private financial data.

Non-profit organizations that support a vast array of societal services face the very same cyber threats as other organizations: ransomware attacks, hacking, data breaches and volumetric distributed denial of service - yet their ability to attract and retain cyber professionals is hampered by both the lack of available talent and constraints in offering market compensation for high-demand jobs.

Additionally, finding qualified teachers and trainers for cyber security courses is difficult, compounding the problem for non-profits, educational organizations, and the industry in general.

**How is the state of Michigan, along with the Merit Network, working to promote cybersecurity education at the K-12 level? What are the challenges and opportunities to cybersecurity education at this level?**

The talent pipeline for cyber security starts in K-12, and it is essential that skill development and awareness of cyber security career opportunities begin at early ages. Given that this field is fairly new and rapidly evolving, there has not been a consistent emphasis in this area for K-12 students or teachers.

Further, the talent pool can be expanded by providing more opportunities and support for under-represented groups, including women and minorities, whose participation in the cyber workforce has been historically low, even though it is clear that much potential exists. By one estimate, women represent only 24% of the cyber security workforce.

It is imperative that we demystify and (to borrow a phrase coined by an executive university colleague in Michigan) "de-nerdify" cyber skills and aptitude for young adults to broaden the appeal of this career path. America needs more cyber defenders to compete and win in this modern digital geopolitical world, and these skills should be recognized and valued by society.

To help promote K-12 awareness and enthusiasm for cyber security opportunities, the State of Michigan engages Merit on an annual basis to conduct the Governor's High School Cyber Challenge. In each of the past few years, we've had over 600 students and over 200 high school teams participate in this challenge - with the top 10 teams being invited to the final contest at the Governor's North American International Cyber Summit in Detroit. The top three teams are awarded trophies by the Governor, and the community pride, excitement and social media activity for local teams is incredible. Through this event, Michigan has discovered and celebrated K-12 cyber talent in every corner of our great state - urban, metropolitan and rural.

With the support of the Michigan Economic Development Corporation, Merit has also expanded our Cyber Range Hubs to K-12, further building the early talent pipeline through a blended learning model that aims to meet the current demand for workforce skills, and to also serve future industry needs.

**Where should Federal and State governments focus future efforts to bolster the cybersecurity workforce pipeline?**

Federal and state governments should focus on:

- Developing the talent pipeline early in K-12, beginning with promoting awareness for both teachers and students;
- Providing financial support for education, training and professional certification, including early certification in high school and college;
- Encouraging cyber skills development for under-represented groups to grow the talent pool, and;
- Incentivizing coordinated efforts between academia, industry and government.

Examples of these strategies might include:

- Increase cyber security career awareness starting in K-12 through the promotion and support for cyber challenges and e-sports, which improve interest in STEM careers;
- Support teacher and faculty professional development in cyber security;
- Expand scholarships for under-represented student groups in cyber-related degree programs;
- Support early credentialing/professional certifications within traditional degree pathways in higher education and within high school programs;
- Subsidize veteran retraining and certifications in cyber security disciplines;
- Incentivize industry internships and apprenticeships in cyber security;
- Promote and maximize the impact of existing federal and state programs where cyber security hasn't traditionally been considered.

merit
NETWORK. SECURITY. COMMUNITY

### *Joseph Sawasky - Bio*

*Joseph Sawasky is currently the President and CEO of Merit Network, Inc., a non-profit corporation governed by Michigan's public universities. Merit owns and operates the nation's longest-running regional research and education network, having been formed in 1966 by the University of Michigan, Michigan State University and Wayne State University. Michigan's public universities created Merit as a shared resource to help meet their common need for advanced networking, and it is currently considered a national leader in this area. In the late 1980s through the early 1990s, Merit operated the National Science Foundation Network, the precursor to the modern Internet. Today, Merit provides high-performance networking, cyber security solutions and community-building services to nearly 400 higher education, K-12, library, governmental, community and healthcare organizations, among others.*

*Mr. Sawasky and his team at Merit have launched a statewide broadband expansion program, called the "Michigan Moonshot", and they are active at the state and national level to help close the digital divide.*

*Merit's altruistic mission is "Connecting organizations and building community". For more information about Merit, please visit https://merit.edu and https://en.wikipedia.org/wiki/Merit_Network.*

*From 2007-2015, Mr. Sawasky was the Chief Information Officer at Wayne State University in Detroit, Michigan. He and his IT organization transformed technology services for the campus – consolidating and modernizing IT, improving the student/faculty/staff experience, and developing award-winning technology innovations. During this time, he also served on the boards of Merit Network, the Detroit CIO Executive Summit, and Michigan Technology Leaders.*

*Mr. Sawasky also worked at the University of Toledo, his alma mater, for 22 years, and in his last position there, served as CIO, leading technology aspects of the unique merger of the University of Toledo, the Medical University of Ohio and its academic medical centers and clinics.*

*Mr. Sawasky resides in Charlevoix, Michigan with his wife, Janis, and is a lifelong resident of the state.*

## TESTIMONY OF MS. SONYA MILLER, H.R. DIRECTOR, IBM SECURITY AND ENTERPRISE & TECHNOLOGY SECURITY

Ms. MILLER. Chairman Stevens, Ranking Member Baird, and distinguished Members, I'm the H.R. Director for both our internal security and for our division that helps clients to protect against cyber attacks. IBM Security is the largest security vendor in the world. IBM manages over 70 billion security events per day for our clients, one of the largest security intelligence operations in the world. We have 17,500 clients in more than 130 countries, 8,000 employees, including researchers, developers, and subject matter experts focused on security, and more than 10,000 security-related patents. Since 2015, IBM Security has hired nearly 4,400 additional experts into the security business and invested more than $2 billion in dedicated R&D (research and development).

Although today's hearing focuses on cybersecurity, the workforce challenges for research are similar. Inclusion, alignment, and attainment are obstacles of both cybersecurity and the research workforce pipeline.

To this end, I would also like to take this opportunity to thank the Committee for its very strong leadership and support of the *National Quantum Initiatives Act*.

Now, to understand IBM Security, it's important to understand the people behind the brand. Our cybersecurity experts have a broad range of skills, including researchers analyzing software for vulnerabilities, incident response teams, analysts who spend hours studying the tactics of cyber criminals, and a security operation center staff who guards us in real time from threats around the globe.

New-collar workers with skills, experience, and diversity but lacking degrees are a strategic opportunity for the cybersecurity workforce. Around 2/3 of the U.S. working-age population doesn't have a bachelor's degree. IBM new-collar approach emphasizes work-based learning and core skills like teaming and adaptability. It is a pathway to finding and attracting nontraditional candidates with diverse backgrounds and skill sets.

To expand new-collar pathways into our cybersecurity jobs, IBM is experimenting with a multitude of approaches to educate and develop the next generation of cybersecurity professionals. Over 220 pathways in technology early college high schools, so P-TECHs, are educating students in 24 countries with the participation of over 600 companies. Through P-TECH, public high school students can earn both a high school diploma and an industry-recognized 2 year postsecondary degree at no cost to them or their families, while working with industry partners like IBM on skills mapping, mentorship, and workplace experiences and internships. IBM launched our apprenticeship program in October 2017. Apprentices are paid while in the program, avoiding that student loan debt and earning skills to work in the tech industry right away.

Finally, IBM is trying to tap into sources of talent that have been underrepresented in cybersecurity. As others mentioned, for example, women are globally underrepresented in the cybersecurity profession at 24 percent, even lower than the IT industry overall. IBM is actively recruiting underrepresented groups through programs that seek underrepresented talent for a more inclusive workforce.

IBM's effort to build a cybersecurity workforce proves to be working. Nearly 20 percent of our security hires since 2015 were new-collar workers. IBM urges the Committee to examine the following areas for change, government activity that will improve the cybersecurity workforce. One, introduce and enact companion legislation to S. 2775, the *HACKED Act of 2019*, as passed by the Senate Commerce Committee, and work closely with your colleagues in the Senate to pass a bipartisan proposal that will strengthen Americans' cybersecurity workforce and align education and training with the cybersecurity workforce needs.

Second, higher education act reforms, including passage of H.R. 3497, the *JOBS Act of 2019*, to extend Federal Pell Grant eligibility of short-term programs, removal of restrictions that prevent students from using their Federal work-study with cybersecurity-related internships in private sector, and support additional pathways to careers.

And third, explore P-TECH models. Federal agencies should explore the P-TECH models for workforce development strategies they can implement and expanding new-collar hiring. The Federal Government should adopt a new-collar approach to real and expanded sources of labor.

So thank you, Members of the Committee, for the opportunity to present IBM's approach to improving cybersecurity education and your consideration of this testimony. I'm looking forward to your questions.

[The prepared statement of Ms. Miller follows:]

**Sonya Miller, HR Director, IBM Security and Enterprise and Technology Security**

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

**February 11, 2020**

**Hearing of**
**the Subcommittee on Research and Technology of the**
**House Committee on Science, Space and Technology**

Chairwoman Stevens, Ranking Member Baird and distinguished Members, I am the HR Director both for our internal security and for our division that helps clients to protect against cyber-attacks.

The House Science, Space and Technology Committee has a critical jurisdiction that supports American technological innovation, research and development, and key agencies to advance U.S. scientific leadership.

Although today's hearing focuses on cybersecurity, the workforce challenges for research are similar. Inclusion, alignment, and attainment are obstacles to both cybersecurity and the research workforce pipeline.

To this end, I would also like to take this opportunity to thank the Committee for its very strong leadership and support of the National Quantum Initiative Act. The NQI is groundbreaking legislation that, once fully implemented, will assure U.S. investment and research in quantum computing remains a priority.

## IBM's Security Capabilities

IBM Security is the largest security vendor in the world. IBM manages **over 70 billion** security events **per day** for our clients – one of the largest security intelligence operations in the world. We have 17,500 clients in more than 130 countries, 8,000 employees, including researchers, developers, and subject matter experts focused on security, and more than 10,000 security-related patents.

Since 2015, IBM Security has hired nearly 4,400 additional experts into its Security business and invested more than $2 billion in dedicated R&D. In sum, we "see" a lot of demand for workforce in cyberspace.

To understand IBM Security, it's important to understand the people behind the brand. Our cybersecurity experts have a broad range of skills including researchers analyzing software for vulnerabilities, incident response teams, analysts who spend hours studying the tactics of cyber criminals, and Security Operation Center staff who guard us in real-time from threats across the globe.

**Challenges Companies Face in Recruiting, Training and Retaining Skilled Cybersecurity Professionals**

Unfortunately, the U.S. education system is not producing candidates with relevant "soft skills" or even the technical skills for jobs in the cybersecurity space except from a narrow swath of students. The pathways through education include many barriers and often leave students with debt but no degree.

**Inclusion:** The distribution of bachelor's degrees is low and uneven by income[1], race, age, and gender[2] (in addition to geography). As a result of the variation, higher education graduates are from a much narrower band of students than the US population.

**Alignment:** Often, higher education institutions simply do not offer cybersecurity majors, minors, degrees, or programs. For example, Michigan State University offers Computer Science or Computer Engineering majors in its College of Engineering, but not cybersecurity as a major, minor, degree, nor program.[3]

Community colleges are offering more and more cybersecurity programs making them an important source of talent. However, fewer than 30 percent of the roughly 1,100 public and independent community colleges across the United States offer a cybersecurity degree, certificate or course.[4]

**Attainment:** The Higher Education Act does not permit financing for programs of less than 600 hours – exactly the type of education pathway that leads to cybersecurity certifications.
Even when a higher education institution offers cybersecurity courses, the bumpy and obstacle-filled pathway of higher education interferes with progress to graduation. End-to-end, only 13% of the 852,439 students who enrolled in community college in 2010 persisted to a

[1] http://www.equality-of-opportunity.org/papers/coll_mrc_paper.pdf

[2] https://nscresearchcenter.org/wp-content/uploads/Completions_Report_2019.pdf

[3] https://reg.msu.edu/Courses/Search.aspx

[4] "2016 Fact Sheet." American Association of Community Colleges. http://www.aacc.nche.edu/AboutCC/Documents/AACCFactSheetsR2.pdf; IBM Institute for Business Value interview with Casey O'Brien, Executive Director & Principal Investigator, National CyberWatch Center. February 21, 2017.

bachelor's degree by 2016.[5] The GAO has found that "students who transferred from 2004 to 2009 lost, on average, an estimated 43 percent of their credits."[6]

For example, in 2012, the Michigan legislature included language in the community college appropriations bill calling for improvement in the transferability of college courses.
But, Michigan Transfer Agreement (MTA) does not address the transfer of their cybersecurity courses from community colleges (such as Schoolcraft) and only protects the transferability of nine non-security related course such as English composition, social science, fine arts and humanities, to name a few.

## Developing Cybersecurity Skills: The IBM New Collar Approach

IBM's New Collar approach focuses on skills first — not degrees earned - and emphasizes work-based learning and core skills like teaming and adaptability. It is a pathway to finding and attracting nontraditional candidates with diverse backgrounds and skill sets.

Around two-thirds of the U.S. working age population does not have a bachelor's degree. Additional education pathways can provide cybersecurity opportunities to the two-thirds of the country that haven't graduated with a bachelor's degree – and those additional students that are ending their education early, with debt but no degree, each year.

IBM Security seeks New Collar employees with learning agility, skills, and experience who will seek continuous lifelong learning and professional growth.

To expand new collar skills, IBM is experimenting with a multitude of approaches to educate and develop the next generation of cybersecurity professionals

**P-TECH** -- Over 220 Pathways in Technology Early College High Schools (P-TECH) are educating students in 24 countries with the participation of over 600 companies. Through P-TECH, public high school students can earn both a high school diploma and an industry-recognized two-year postsecondary degree at no cost to them or their families, while working with industry partners like IBM on skills mapping, mentorship, workplace experience and internships.

The P-TECH model of schools has four key elements:

- Alignment of the Program of Study for grades 9-14 with the skills needed by an employer
- Mentors for all students from the employer
- Internships for students from the employer

[5] https://nscresearchcenter.org/wp-content/uploads/SignatureReport13_corrected.pdf
[6] https://www.gao.gov/products/GAO-17-574

- A commitment that graduating students will be first in line for a job with the employer.

Apprenticeship: IBM launched our Department of Labor Registered Apprenticeship Program in October 2017. It's a program for the 21st century, focused on building skills in cybersecurity, data scientist, software development and more. This 12-24-month program pairs apprentices with an IBM mentor to work on actual IBM projects, along with traditional classroom learning, in technology's fastest-growing fields.

Apprentices are paid while in the program, avoiding student loan debt and earning the skills to work in the tech industry right away. We hired as many as 500 apprentices by the end of 2019, and we expect to hire 450 apprenticeships each year moving forward for the next five years with some being in such roles as cyber security analyst and hardware hackers. Apprenticeship programs are great opportunities for mid-career workers to build new skills or break into new industries without having to leave the workforce to be a full-time student. It's a chance to earn while you learn.

Outreach: Women are globally underrepresented in the cybersecurity profession at 24%, much lower than the representation of women in the overall global workforce. In 2016, women in cybersecurity earned less than men at every level.[7] IBM is actively recruiting underrepresented groups through conferences and organizations like the International Consortium of Minority Cybersecurity Professionals (ICMCP), the Grace Hopper Celebration and Women in CyberSecurity (WiCyS).[11] Additionally, we have an internal network called Women in Security Excelling (WISE), an IBM professional development community that also sponsors and hosts external events like the "Cyber Day for Collegiate Women" programs for college women.

IBM's efforts to build a cybersecurity workforce prove to be working – as mentioned, we have built a business of over 8,000 experts including an additional 4,400 since 2015 – although job openings at IBM Security are still plentiful. That workforce is a result of reaching new sources through our New Collar recruitment – in fact, nearly 20% of our security hires since 2015 have fit into this "new collar" category.

**What Should the U.S. Government do to Address Cybersecurity Skills and Capabilities?**

IBM urges the Committees to examine four areas for changed government activity that will improve the cybersecurity workforce. Those four areas are listed below and then discussed in more detail:

[7] https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf [11] International Consortium of Minority Cybersecurity Professionals website, accessed April 3, 2017. https://icmcp.org/; Women in CyberSecurity website, accessed April 3, 2017. https://www.csc.tntech.edu/wicys/

- **Introduce and Enact Companion Legislation to S. 2775, the HACKED Act of 2019** as passed by the Senate Commerce Committee, and work closely with your colleagues in the Senate to pass a bipartisan proposal that will strengthen America's cybersecurity workforce and align education and training with the cybersecurity workforce needs.
- **Higher Education Act Reforms** including Passage of the HR 3497, the JOBS Act of 2019 to extend federal Pell Grant Eligibility of Short-Term Programs, removal of restrictions that prevent students from using their Federal Work Study with cyber-related internships in the private sector and support additional pathways to careers.
- **Explore P-TECH Model** -- Federal agencies should explore the P-TECH model for workforce development strategies they can implement.
- **Expand New Collar Hiring** -- The federal government should adopt a New Collar approach to reach and expand sources of labor.

**Introduce and Enact S. 2775: The Hacked Act of 2019.** Multiple education pathways to cybersecurity careers are a goal of IBM and central to the HACKED Act. Under the legislation, the Director of NIST is directed to target identified skills gaps and ensure that existing education programs, partnerships, and regional alliances lead to specific tasks found in the NICE Cybersecurity Workforce Framework. Our experience with P-TECH has shown that collaborations with government, education systems, and employers are very productive.

The Hacked Act will facilitate: "local and regional partnerships—

> (A) to identify the workforce needs of the local economy and classify such workforce in accordance with such framework;
>
> (B) to identify the education, training, apprenticeship, and other opportunities available in the local economy; and
>
> (C) to support opportunities to meet the needs of the local economy.

IBM is strongly supportive of these goals due to our experience with P-TECH and apprenticeships.

**Higher Education Act Reforms including Passage of HR 3497, the JOBS Act of 2019 and other additional pathways.**

IBM urges the House to move remove obstacles in the Higher Education Act to inclusion, alignment, and graduation by allowing students to use their Pell Grants for shorter education programs that lead to certifications. Under existing law, students who need short-term programs of 150 to 600 hours length in order to get certifications are required to sign up for longer education programs or forgo federal financial assistance.

- <u>We want the Pell grant program</u> to allow part-time students and mid-career professionals to get financial support to acquire new skills — including certifications, apprenticeships, other job-related classes. Pell Grants need to work harder for everyone with need, not just full-time students.

- <u>Education pathways should be revised so grants and loans can support more career pathway opportunities. Student aid should support the attainment of degrees *and* the attainment of industry recognized credentials and licenses, and</u> support apprenticeships, certificate programs, or other mid-career re-skilling.

- <u>We want the federal Work-Study Program revised to</u> remove restrictions on student use of funds for off-campus work experiences like internships at companies. These funds should not be restricted to supporting jobs in campus cafeterias and libraries.

<u>**Explore P-TECH Model Participation by Federal Agencies:**</u> The P-TECH model is based on a collaboration between employers and educators to improve alignment of the existing education system with needed job skills. Developing programs of study and educational materials is the responsibility of our nation's educators, but P-TECH employers play a vital role by telling what skills are necessary "to be first in line for a job". Defining skills needs, providing mentors, internships, and committing that graduates will be "first in line for a job" are all employer responsibilities in the P-TECH model.

Federal agencies are major employers and should explore the workforce development strategies developed and tested by the private sector through the P-TECH model schools. Federal agencies could join other P-TECH employers that provide information to workforce boards and educators on needed-job skills. Federal agencies could provide work-based learning opportunities including mentors and internships. Both student and potential federal employers benefit from enhancing skills learned through improved alignment and work-based learning.

<u>**New Collar Approaches:**</u> Finally, IBM recommends that "Skills First" approach to recruitment expand the New Collar cybersecurity workforce. For a more robust New Collar approach, employers need to create new collar career pathways in their workforce strategy with five components:

- Agility Centered Recruitment
- Skill Maps
- Broader Recruitment
- Education Ecosystem
- Work based Learning
- Retention

With an expanded recruiting aperture bringing new talent in, there must be comparable efforts to work to retain the talent. Keep employees engaged by providing opportunities for them to advance and keep skills up to date through classes, certifications, conferences. Cybersecurity is a highly dynamic field, which requires a constant refreshing of skills. Additionally, support existing New Collar employees from other functions who want to move into cybersecurity as a new career.

**Conclusion**

With the four approaches above, IBM believes New Collar workers can add an important component of the nation's overall approach to tackling the cybersecurity skills gap. It is applicable across industry and government and has tangible benefits for both employers and potential employees. By not tapping into underutilized sources of talent across the country and supporting and nurturing it, we are doing a disservice to everyone and not securing ourselves as well as we could. There are many innovative approaches to improving cybersecurity education happening all across the country, but to truly address the cybersecurity skills gap we need to scale these approaches, including new collar ones.

Thank you, Members of the Committee for the opportunity to present IBM's approach to improving cybersecurity education and your consideration of this testimony. I look forward to your questions.

## Biography

### Sonya Miller, HR Director, IBM Security and Enterprise and Technology Security

Sonya Miller is the IBM HR Director for both IBM Security and Enterprise & Technology Security (E&TS) – two distinct divisions within IBM that require workers who have the skills and experience in cybersecurity needed to protect IBM and our clients. IBM Security is an ever-growing business unit and E&TS is responsible for managing the cybersecurity landscape and protecting both IBM internal systems and the delivery of secure products and offerings to our clients. In my position, I am charged with ensuring both divisions have the skilled staff needed to fulfil their important missions.

IBM Security is the largest security vendor in the world. IBM manages **over 70 billion** security events **per day** for our clients – one of the largest security intelligence operations in the world. We have 17,500 clients in more than 130 countries, 8,000 employees, including researchers, developers, and subject matter experts focused on security, and more than 10,000 security-related patents.

Since 2015, IBM Security has hired nearly 4,400 additional experts into its Security business and invested more than $2 billion in dedicated R&D.

Chairwoman STEVENS. Well, we've done a few things in this space, and you all touched on some great points.

At this time, we'd like to open up for 5 minutes of questioning. And the Chair is going to recognize herself for 5 minutes of questioning, so we can start the clock now.

You know, certainly we've taken some steps just in the last couple of weeks with Chairwoman Johnson's support. We launched the first-ever Women in STEM Caucus in Congress. Dr. Baird and I got a bill signed into law at the end of last year, the *Building Blocks of STEM Act*, which is, again, supporting those early childhood investments in educational programming for science, technology, engineering, and mathematics. And that continuity, as we all know, is so important, right, that onramp, the pathways. Your testimonies all specifically touch on that.

Mr. Petersen, I just wanted to—let's understand a little bit about—more about NICE here, NICE within NIST within the Department of Commerce. How big is your department?

Mr. PETERSEN. So we are a small team of five full-time employees, and we have an approximate $4 million budget appropriated by Congress, so a relatively small organization.

Chairwoman STEVENS. OK. Great. Well, we'll be going through the budget reauthorization and taking a look at that and making sure—so the—just the—half—less than half a dozen of you developed the CyberSeek tool or did you contract out for that?

Mr. PETERSEN. So that was a grant given to——

Chairwoman STEVENS. OK.

Mr. PETERSEN. [continuing]. CompTIA and Burning Glass to actually——

Chairwoman STEVENS. Oh, Burning Glass.

Mr. PETERSEN [continuing]. Develop the tool. Yes.

Chairwoman STEVENS. OK. Burning Glass. Oh, they're great. They're fabulous. Well, that's a big accomplishment. And we're glad to share that today, and we'll continue to share that.

And is that on the NICE website? Is that——

Mr. PETERSEN. There's a link to it, but it's——

Chairwoman STEVENS. OK.

Mr. PETERSEN. [continuing]. CyberSeek.org——

Chairwoman STEVENS. CyberSeek——

Mr. PETERSEN [continuing]. You can find it.

Chairwoman STEVENS. CyberSeek.org. OK, great.

And as part of that heat-mapping process and, you know, as we look to get in front of this, we—and, Ms. Miller, you probably know this all too well, which is that the job profiles are always changing, right? So we're seeking to hire for certain roles. We know we have an emphasis on cybersecurity, but with IOT (internet of things), other advancements, you mentioned quantum, the nature of the work is changing. Have any of you explored or seen how job profiling, taxonomy work, maybe in—you know, with some of the big placement agencies, Manpower, Kelly Services in Michigan, has that impacted this cybersecurity workforce skills gap that we're experiencing? I don't know if, Ms. Miller, you wanted to chime in there.

Ms. MILLER. Well, IBM, we provide several assessments to candidates around personality, so it's testing for the softer skills, as well as learning agility, so a propensity toward lifelong learning. So instead of testing for a specific job, we're really looking for these kind of softer skills, as well as some level of technical capability. So, you know, jobs—there's jobs now that didn't exist 10 years ago. Therefore, you have to have that agility in how your assessing people. You can't just assess them for the job at hand.

Chairwoman STEVENS. Yes. And, Mr. Sawasky, are you seeing this, you know, the talent qualifications as described—you're working hand-in-hand with the universities and have this great career in this space, but the job profiling here I also think is something that we want to kind of match up so that, you know, when we're entering into the workforce, we've got that pipeline and access.

Mr. SAWASKY. Yes, absolutely. You know, I think what we're looking for are problem-solvers and pattern-finders here, regardless of sort of academic discipline. Some of the finest IT professionals I've ever worked with were anthropologists and psychologists and others.

Chairwoman STEVENS. Yes.

Mr. SAWASKY. So it's not absolutely necessary that computer science is, you know, the first part of the background for a successful career in cyber.

Chairwoman STEVENS. Great. Dr. Siraj?

Dr. SIRAJ. So, you know, if you go to the CyberSeek website, there is also an interactive pathways tab. And if you click on that, it shows that in reality most of the data shows that the top jobs are all based on computer science. But, you know, it is absolutely true that cyber is very multidisciplinary. And then we can have people coming from all walks of life to have something—I mean, everyone can contribute to solve a problem in cyber because cyber is so vast.

Plus, also, you know, the NIST/NICE workforce framework also helps with that because in that framework Department of Homeland Security actually gave out a tool where someone can go in and say, OK, I'm interested in data base, and it will show that student or that person, you know, where in the NIST framework that this person can contribute to in what way.

Chairwoman STEVENS. Yes.

Dr. SIRAJ. Again, cyber is something that anyone can contribute to with their own skills.

Chairwoman STEVENS. Right. And so, Mr. Petersen, I'm sure some of this is resonant with you. Do you see NICE being able to work with every one of our witnesses and their portfolio of work? And would our witnesses also agree that you get a lot out of working with NICE and that department? So this five-person department in the, you know, Department of Commerce, NIST——

Mr. PETERSEN. Yes, I was going to comment even though we have five team members, the NICE community is vast and everybody——

Chairwoman STEVENS. Yes.

Mr. PETERSEN [continuing]. On the stage, every organization represented here has worked directly with NIST and NICE in the past in our national efforts. So our——

Chairwoman STEVENS. Leveraged partnerships.

Mr. PETERSEN. Absolutely.

Chairwoman STEVENS. Great. Thank you. I'm slightly over. I'm going to yield back the rest of my time and recognize my colleague Dr. Baird for 5 minutes of questioning.

Mr. BAIRD. Thank you, Madam Chair. And, you know, I've gained a great deal of insight just having you here today, and I'm sure those that are listening and read the reports will also feel the same way.

But, Ms. Miller, I see in your testimony you said you handle 70 billion security events per day for your clients? I mean, that——

Ms. MILLER. Well, not me personally, yes. IBM Security does.

Mr. BAIRD. I understand. So then I have an interest in veterans, and so they bring a wealth of skills from their military training and then they got a lot of hands-on experience. Sometimes they're not able to transfer their military training over into various programs. So I guess my question is what's IBM doing in their new-collar program? Is that applicable to veterans? And then the second part of the, have veterans participated in this program?

Ms. MILLER. Yes, absolutely. So we have a variety of programs targeted to veterans because they tend to actually be a very good fit for cybersecurity roles, whether they've worked in cybersecurity while in the military or they got requisite training once they've left the military. We have a Veterans Employment Initiative, so that's free training on IBM software. And it comes with a certificate at the end. We touch over 100 veterans per year with that program using IBMers donating their time.

We also have a corporate partnership with the USC Marshall School Masters of Business for veterans, so we have IBM mentors, advisors, and SMEs (small and mid-size enterprise) donating their time to work with the veterans on capstone projects, so basically developing innovative solutions to real-world issues.

And, finally, we're also hiring veterans at all levels in the company and in the security organization. I actually in January was down in Austin, and we have a cohort of apprentices that started in the first quarter of last year. Fifty percent of those apprentices are veterans. One actually worked in cybersecurity while in the military, and then applied through the apprenticeship program what's going private sector. Another one actually left the military. He worked for 10 years as a corrections officer, decided to use some of his military benefits, and now he's in our apprenticeship program. They're hardware hackers and they're doing excellent.

Mr. BAIRD. Super. Then my next question goes to all of you. You know, I mentioned earlier that Indiana has got four Cybersecurity Centers for Academic Excellence, and I'm having fun with the Chair about Indiana and Michigan, but in reality I'm just using them because I'm familiar with it. So the question comes down to how the Federal Government can further build on programs like they have at Purdue, and someone mentioned more like a 2-year program and so on. So I guess I'm just asking how we as the Federal Government giving you the opportunity to expand on how you think we can be helpful in that area and to fill the half million jobs we have?

And so this is going to be ladies first. Dr. Siraj, you go first, and then Ms. Miller and then back to Mr. Petersen.

Dr. SIRAJ. So, you know, as I said in my testimony that programs like the CAE program that is NSA DHS program—programs, NSF programs like CyberCorps, DOD (Department of Defense) program like Cybersecurity Scholarship, GenCyber program, I mean, all of these programs have been so impactful to—I think the best thing about these programs is that it enables smaller schools to have resources to build an army on the ground. And then, you know, once we have all these institutions making change in their own community, then collectively we are going to see so much in the Nation.

So, you know, empowering these programs, again, NIST/NICE has been extremely crucial for universities to get the momentum going and also commissioning more programs like this that looks at how to train educators in cybersecurity because that is the biggest challenge. In 2018 there were 114 Ph.D.s in cybersecurity, and only 14 of them went to universities as faculty. So if we want to build pipeline in universities for students, we have to find some ways to train and prepare and allow educators to go into universities.

Mr. BAIRD. I see I'm over on time. Is it all right if——

Chairwoman STEVENS. Yes, of course.

Mr. BAIRD [continuing]. They go ahead? Go ahead.

Ms. MILLER. OK. I'll be quick. The *Higher Education Act* I talked about reforms there, really removing the obstacles on how people can use the funding students so that they're not pushed into having to go through a 4-year degree. So I talked about work-study programs and using their benefits to work in the private sector in the field that's relevant for their career aspirations, as well as using Pell Grants for shorter education, you know, certifications and things like that versus the 4-year degree I think is really important where we really could use some help there to help students.

Mr. PETERSEN. So I think what NICE and NIST is best at is convening communities, and so a lot of our work is at the national level. We actually convene an annual K–12 conference to bring together K–12 educators and administrators from across the Nation. We do our own annual NICE conference that brings together industry, academia, as well as government. We also collaborate internationally. There's quite a few other countries that are interested in adopting the NICE Cybersecurity Workforce Framework as a standard not only for their country but because of the global nature of work.

But we fundamentally believe that a lot of the solutions and the answers are in the local communities, whether it be a State like Michigan and the ecosystem that Mr. Sawasky described is exactly what we promote in Indiana and all of your different States, or at the local level, regional level, however that might be defined. So when I earlier described that RAMPS for Cybersecurity Workforce Development, that's really about regional alliances, getting the K–12 higher education training ecosystem working together to meet local workforce needs.

Mr. SAWASKY. I think fundamentally we need more funding to grow the, you know, cybersecurity workforce than we have now. I listened to my colleagues talk about, you know, graduating hundreds of cyber pros at a time. And really we need to be looking growing them at thousands at a time.

And the notion of early credentialing, building on what Ms. Miller said, is really important. I will let you know that my son Jerrod was pursuing his bachelor's degree in computer science, and I strongly urged him to obtain a professional cybersecurity certification in his sophomore year, and he did that. And he got a job, and he's actually paying for his own school now. He's out of the house, which is nice as well. And he is becoming very successful with that early credentialing program, and allowing students to support that early credentialing in formal—in normal degree pathways I think is really important.

Mr. BAIRD. Thank you. And I yield back.

Chairwoman STEVENS. Great. And at this time we're going to recognize Ms. Johnson for 5 minutes of questioning.

Chairwoman JOHNSON. Thank you very much.

I guess I can direct this to each of you. What are the major challenges that have led to the cybersecurity workforce shortfall? And what should Congress focus its future efforts on to bolster the cybersecurity workforce?

Dr. SIRAJ. OK. So I will start. I think K–12 is the, you know, most impactful because there is really not so much activity in cybersecurity at K–12 and computer science. There are only 33 States now that have started to have some programming in computer science, and cybersecurity is much, much behind that. So preparing teachers in K–12, you know, provide opportunities to students like high school students, giving them internships in cybersecurity, doing partnership with educational institutions, giving infrastructure to K–12 so that—you know, there is a trend right now that K–12 schools are being hacked, so they need to also, you know, strengthen their infrastructure.

And, again—so that's K–12. And in postsecondary there is so much to do. Not many schools offer cybersecurity courses. I think the key thing is to—not to treat cybersecurity as a silo but integrate in computer science education, in STEM education. In fact, make it a general education course in universities.

Mr. SAWASKY. I think awareness is really important. A lot of children in K through 12 aren't even aware that cybersecurity is an option for careers. And I think in Michigan with our Governor's Cyber Challenge, that's really helped promote that awareness, too. And it's been fun to watch people who traditionally haven't thought about career opportunities in that field really dig in and work with their teachers and local coaches.

And Merit being a network provider offers as a cloud-based service so that we can reach every corner of our State into underserved areas like Detroit and to rural areas like Marquette, Michigan. We've seen talent emerge from those programs.

Ms. MILLER. So just to kind of build off of that, so 2/3 of high school students said the idea of a career in cybersecurity had never been mentioned to them by, you know, teachers and guidance counselors, so there's one of our problems is that, you know, again, it's not being mentioned. It's not being thought about while they're in school.

One of the things IBM is doing focusing on this is we actually have something called IBM Cyber Day for Girls where we have some of our professionals in cybersecurity at IBM go out and meet with middle school girls to tell them about careers in cybersecurity, as well as go through kind of a workshopping day where they, you know, teach them about IOT, cybersecurity hygiene, and those types of things to hopefully get them more excited about cybersecurity. So we're trying to, you know, kind of kill a couple birds with the same stone by getting women or girls more interested in cybersecurity, as well as educating about cybersecurity.

I also mentioned was we do need more curriculum—strong curriculum in community colleges and 4-year colleges around cybersecurity. Many do not have majors, minors, or any kind of program study and certificate that they can get in those areas, and I think that's going to be important as we continue to move on and focus on the skill set.

Mr. PETERSEN. And while NICE would certainly agree with everything that's been said and career discovery being critical, I would say in addition to young people, we need to focus on working adults. We need to focus on the transitioning veterans, veterans' spouses, military spouses, adults that are underemployed, unemployed, opportunity youth who are in that 18 to 25 age group who aren't currently getting an education or working in a job because that's going to be the long-term solution. But we have an immediate shortage today, and we have to focus on adults as well as young children to have both a near-term as well as a long-term solution.

Dr. SIRAJ. Also if I may add, community college is a big part of the conversation because they represent the most diverse body of students, so we must find effective ways to create pathways from community college to 4-year universities or find ways to get this community college students into industry because there are—you know, there aren't many jobs that will accept community college students with associate degrees in cyber.

Chairwoman JOHNSON. Thank you very much. My time is expired.

Chairwoman STEVENS. At this time we're going to recognize Dr. Foster for 5 minutes of questioning.

Mr. FOSTER. Well, thank you. I'd like to speak about—the Department of Homeland Security oversees a program called Cybersecurity Education and Training Assistance Program, or CETAP, that's run by the National Integrated Cyber Education Research Center pronounced NICERC. Now, CETAP promotes cybersecurity education at multiple grade levels in multiple States, including Illinois. It provides Federal financial assistance toward community-based efforts to increase knowledge of cybersecurity topics and to encourage interest in cybersecurity as an academic pursuit and as a professional career.

CETAP has hosted professional development workshops in both Joliet and Aurora in my district, and Joliet and Aurora teachers have attended professional development workshops hosted by Chicago State University. Unfortunately, it's my understanding that the latest President's budget has zeroed out this program once again.

Now, Mr. Petersen or anyone else on the panel, could you describe the CETAP program and curricula and what makes it successful?

Mr. PETERSEN. So I am directly familiar with the NICERC program, as you describe. And as I just said earlier, we support a pretty broad, vast community and I'm proud to say NICERC is very actively engaged with us and us with them as well. For example, they are regular participants and sponsors at our K–12 Cybersecurity Education Conference, which brings together educators and administrators from across the Nation. And, as you described, many States, many school districts, and many State Departments of Education are using their curriculum. And it's a way to get cybersecurity, as we heard described earlier, into the schools at a younger and younger age. So we certainly appreciate the effort they've done to both raise awareness and the need to integrate cybersecurity across the curriculum in our K–12 schools and the way to kind of distribute the work that needs to be done across the United States by developing a common curriculum that they're trying to introduce in multiple States.

Mr. FOSTER. Yes. So are there many other curricular—curricula-based programs for K–12, or are they mainly boot camps?

Mr. PETERSEN. So curriculum happens in a lot of different ways. I mean, for example, at the high school level there's career technical education programs or CTE programs, and there's career technical student organizations, as well as other nonprofits that are partnering with the schools to both develop curriculum, as well as to develop programs of study that the students can pursue to become specialized or more aware of cybersecurity curriculum.

I would say it's an emerging area, which is why NICERC has certainly made an impact in both the number of teachers, as well as number of students reached, but it is an emerging area of opportunity for curriculum development at the K–12 level, as I think we heard Ms. Miller describe.

Dr. SIRAJ. So if I may add, the—I have seen firsthand the impact of NICERC, and what NICERC does, it trains the teachers and not just, you know, computer science teachers but teachers teaching math, arts, sciences, STEM subjects, and it gives them resources so that they can talk about and teach security in their classes. So programs like that, I mean, I think they're crucial for the success of K–12 cybersecurity education and, you know, I cannot say more better things about that program.

Mr. FOSTER. We have an interesting situation in just STEM generally that young women are outperforming young men all the way through the end of high school in STEM fields, and then in the first couple years of college, participation is dropping off dramatically. I just—you know, when I go to robotics competitions in my district, which I do all the time, what I—what I'm told is that all the way through junior high schools the—girls and boys are well-integrated, and then when you hit high school for some reason the gender disparity emerges. What—where—what's the situation in cybersecurity?

Dr. SIRAJ. So, as I stated before, in a couple of years back it was 11 percent. Now, it's 20 percent. It needs to be 50 percent because, as we all know, diverse groups are—outperform any homogenous groups.

But I think what's happening is, as young girls are getting into high schools and colleges, what's preventing them to be in cyber is the stereotypical image that cyber portrays. You know, when you tell a young girl that, you know, if you go into cyber, you're just going to work in a dungeon. That doesn't, you know, sound very promising. But if you tell the young girl that if you work in cyber, you're going to keep peace in cyberspace, you're going to prevent chaotic situations in our modern-day technological lives, that's speaks a lot. So I think the lack of community, the lack of inclusive environment, the lack of role models——

Mr. FOSTER. Yes, the role models is something I've been told repeatedly in things like robotics competitions. For some reason most of the coaches in robotics teams in junior high school tend to be women, and then that's not true in high schools. And so the role models may be difficult to calculate, but it may be a huge effect.

Anyway, Madam Chair, if it's possible if—to have a second round of questions, I would—I would appreciate it if that's feasible.

Chairwoman STEVENS. So we were going to have the—before we brought the hearing to a close, we were going to have the witnesses, as we're here in Congress, share a couple of minutes. But what we can do, Dr. Foster, is open it up for a second round. I'll claim my 5 minutes and cede them to you.

Mr. FOSTER. Very well. So you've done so?

Chairwoman STEVENS. Yes.

Mr. FOSTER. All right.

Chairwoman STEVENS. So I've yielded my time——

Mr. FOSTER. Well, thank you.

Chairwoman STEVENS [continuing]. To my colleague.

Mr. FOSTER. I appreciate it.

I'd like to raise the issue of foreign workers in cybersecurity. In 1980 just 7.1 percent of American computer science jobs were occupied by foreign-born workers. That grew to about almost 30 percent by 2010 because of the breakneck growth in the tech sector, which became increasingly reliant on high-skilled visa-holding immigrants. And, unfortunately, President Trump's immigration policies have made it harder for tech companies to bring highly skilled workers into the United States. For example, in March 2017 the USCIS (United States Citizenship and Immigration Services) announced that entry-level computer programmers would no longer automatically qualify to apply for the visa programs and—but instead of this meaning that more jobs will actually be filled by Americans, it has turned out that it's just more likely now that companies will send the work overseas where there are, you know, employees that are eligible to work. The problem is that there just are not enough trained Americans to fill the growing demand of computer jobs generally.

So in response to this, last year, I introduced the *Keep STEM Talent Act* to provide permanent resident status to international students who completed advanced STEM degrees in the U.S. institutions and they're interested in continuing their research in the United States. I believe we should be encouraging these young scientists to remain in the United States and join the American scientific and cybersecurity workforces.

So, Ms. Miller, how reliant is IBM on foreign talent and computer scientists, and are there instances when you've actually had to move work offshore simply because of the shortage of cyber talent in the United States?

Ms. MILLER. Well, IBM Security specifically is operating in over 130 countries, so we have talent all over the world. We do rely to some degree on bringing talent into the United States, but it could be everything from the experience, you know, so cross-training or the experience that they bring from someplace else to train people here, or we're grooming them and we're—you know, they go back to their home country. So there's a variety of reasons why we may rely on it.

I don't think we have an overabundance of reliance on that, but that's one of the reasons why in the United States we're so focused on the skills-first approach to really bringing in more cybersecurity professionals from here, grooming that talent, providing a lot of resources to help—free resources, curriculums on badges, external digital badges, and the people can—people can attain to demonstrate their proficiency and other tools so that we have the talent here and we're continuing to groom that talent. So that's our main focus. It's not to bring the talent from other countries necessarily but to grow the talent here. And the new-collar approach that we're taking is helping us do that.

Mr. FOSTER. Now, if you look at future needs in cybersecurity, you know, something like half of all cybersecurity instances have to do with someone impersonating someone else online. And so then a lot of the reason that you're focusing on soft skills is to train people simply to operate their authentication properly. And there are interesting proposals out there that the Federal Government allows citizens who wants a means to digitally authenticate themselves online—so this would—in its simplest form would be simply, you know, if you get a Real ID card, you're also given a digital means to assert that ID.

And so that is something that I know a lot of industries are enthusiastic about being able to add onto as part of the way of making sure that you don't have identity fraud, which is, you know, the biggest single component of cyber insecurity in our country. And so this is going to have a big impact if people have good technical means to authenticate themselves. And is that going to really change the nature of the cybersecurity workforce so that you'll be more focused on, you know, device security, program security rather than training people to feed the systems properly?

Ms. MILLER. I'm not sure I'm qualified to actually comment on that. What I will tell you is that in the cybersecurity space cyber criminals, they continue to evolve, and it's hard to keep up with them. We were kind of joking yesterday that we wished we understood the workforce strategy of these threat actors and how they're findings such, you know, great talent that's out there making us have to keep up, making us have to continue to chase and understand what they're doing. But I can't comment specifically on what technology and the effects——

Mr. FOSTER. Well, that's what makes it so tough for STEM training generally. You know, I think 15 years ago we were trying to teach all kids to learn HTML so they could, you know, maintain their own webpages, and now, you know, we've got 3 billion webpage maintainers who maintain their Facebook page, and it's—the nature of technology is that the training is when you're planning 15 years out.

Now, just a last point if I could about the national labs. You know, as I mentioned a few times on this Committee, I'm a proud Co-Chair of the National Labs Caucus, and we're visiting all 17 of the DOE (Department of Energy) labs. We just finished visiting Oak Ridge National Lab. So, Dr. Siraj, in your testimony you highlighted that Tennessee Tech University faculty and graduate students have been conducting research with the scientists and engineers at Oak Ridge National Lab and on various DOE-funded research projects. Could you just say a few words about that?

Dr. SIRAJ. So the way it came about because, you know, Oak Ridge National Lab is just 1 hour away from us, and so we have a couple of faculty in computer science who are working with a couple of groups in Oak Ridge National Lab to work on security research projects that I mentioned in my testimony. Plus, we also have partnership where professionals there who don't have a Ph.D. degree, they're working, they're going into doctoral studies at our school, and our faculty are also going there to teach security classes. There are professionals also coming to our campus to teach security classes.

But, you know, this partnership is, you know—it's a win-win situation for both entities, for the national lab and for us for our students. It provides, you know, big opportunity to speak to the scientist and the role models and learn from them because, you know, what professors know, so——

Mr. FOSTER. Yes. Well, you know, one of my favorite events of the year is to go to Argonne National Lab in my district, which hosts the DOE-sponsored cybersecurity contest where the——

Dr. SIRAJ. Yes, CyberForce competition.

Mr. FOSTER. CyberForce competitions where college teams come in from all over the country and try to hack each other's——

Dr. SIRAJ. Yes.

Mr. FOSTER [continuing]. Equipment and it's——

Dr. SIRAJ. So——

Mr. FOSTER. It's a lot of fun. And, you're right, they do enjoy interacting with the——

Dr. SIRAJ. Yes, so——

Mr. FOSTER [continuing]. Scientists there. Anyway, my——

Dr. SIRAJ [continuing]. Our students do that, too.

Mr. FOSTER. I think my time is expired, so I will yield back.

Chairwoman STEVENS. OK. Dr. Baird, you'll be recognized for 5 more minutes of questioning.

Mr. BAIRD. Mr. Petersen, last May, President Trump issued America Cybersecurity Workforce Executive Order, which directed the Secretary of Commerce and the Secretary of Homeland Security, along with the heads of other appropriate agencies, to implement the recommendations from their 2017 report on how to support growth and sustainment of the Nation's cybersecurity workforce in both the public and the private sectors. So could you tell us if you're involved in implementing these recommendations, and if so, how? And are these recommendations informing the development of NICE's strategic plan for the next five years?

Mr. PETERSEN. Yes, thank you for that question. We are absolutely involved, as we were in both the development of the recommendations, as well as the implementation. There were five imperatives, multiple recommendations and actions, and we are beginning by prioritizing some of them. So, for example, the first one spoke to having a national call for action to make sure that both the public and private sector were recognizing the importance of cybersecurity.

And by way of example, another reason that I've worked closely with IBM is several companies have come together as part of the Aspen Cybersecurity Group to issue a set of principles that they want companies to follow. And one of those principles is to use the NICE Cybersecurity Workforce Framework, but other principles are things like career discovery or doing skills-based hiring and the like. And so working collaboratively with the private sector and industry in this case to raise the importance and elevate this is one way that we are implementing it.

When I talked earlier about transforming the learning process, including more of a focus on skills and less than just traditional credentials, that's another example of an emerging theme in our next strategic plan. We're learning, as many of you have described, it includes not only the K through 12, the high school diploma, the community college, college degree, but also certifications or apprenticeships or the other multiple pathways to a career in cybersecurity.

And finally, as I indicated, the Workforce Policy Advisory Board, which is part of that President's National Council on America's Workforce, will be talking more about the multiple pathways to all types of careers but cybersecurity especially where it could be that transitioning veteran that you described earlier that after a 20-year military career, then enters cybersecurity, or it could be an IT worker who's going to transition to a cybersecurity role. So we are actively working on both prioritizing and implementing them to the extent that we can.

Mr. BAIRD. Thank you. Ms. Miller, one last question. Maybe, could you elaborate on how IBM has utilized their apprenticeship program and how you use that to recruit and retain cybersecurity workforce?

Ms. MILLER. Sure. So we started the apprenticeship program about four years ago, and what we do is we've actually—especially in the security—the cybersecurity organizations have really looked at what are the right roles that we can really bring in talent without the 4-year degrees, so looking at the soft skills, making sure that they have those right critical skills, and leading with skills first and the capabilities over the credentials, right? And then looking at what are the right roles to bring them in, so a security operations center analyst is one, pen testers, another example, technical writers.

We've been bringing people in into those types of positions as a way to, one, test them, make sure that they can—that they have the technical capabilities as we continue to train them up, sponsor them for certifications, et cetera. So as they come in, there is a curriculum that's built out for the first year for them that they go through and dedicated resources to support them. So it's really looking at this from a skills-first basis, and it allows us to get the—you know, those that have 4-year degrees, they tend to not be representative of the overall U.S. population demographically, right? So if we're able to bring in and really leverage the P-TECH programs, the apprenticeship programs, et cetera, we're able to get into—tap into that underrepresented talent, whether it be based on race, gender, even veterans, et cetera.

So this is definitely a way that—and the question was asked earlier. This is a way that in the future people will be able to look up and see people that look like them at the top of the house. So it's very important to us.

Mr. BAIRD. Thank you. And I see I'm out of time. I yield back.

Chairwoman STEVENS. Thank you. And now we'll recognize Dr. Lipinski for 5 minutes of questions.

Mr. LIPINSKI. Thank you, Chairwoman. Thank you for holding this hearing. We all know how important this issue is. And, unfortunately, it doesn't receive nearly as much attention as it should.

I'm happy to follow the Democrat before me, Bill Foster. We share Argonne National Lab, and appreciate the great work that's being done there on cybersecurity.

One particular issue I have is how medium and small manufacturers struggle to keep up with the rapid evolution of cyber attacks. It's something I hear about all the time from these manufacturers in my district.

I was the Democratic lead on the *NIST Small Business Cybersecurity Act*, which was signed into law in 2018. The bill directed NIST to develop voluntary guidelines to help small businesses identify, manage, and reduce cybersecurity risks. NIST has since developed the Small Business Cybersecurity Corner to provide resources on this topic to small businesses. So I want to ask Mr. Petersen. Can you describe the National Initiative for Cybersecurity Education's contributions to these resources for small businesses?

Mr. PETERSEN. Thank you for that question. So we actually have one of our team members, from our small team, that is assigned part-time to help support the small and medium business outreach. One is because her regular role with NICE is to do industry engagement. And again, we want to be sensitive to both the needs of large enterprises, as well as small and medium businesses. So she can bring both that expertise, as well as kind of introduce workforce and education-related topics into that small and medium business outreach.

The reality is we talk about a small team like my own, the small and medium businesses have smaller teams especially devoted to IT and cybersecurity and are often reliant on third-party providers, service providers as well, so making sure that, for example, our NICE Cybersecurity Workforce Framework doesn't just speak to the kind of workforce they need but the kind of workforce that service providers need to bring to them as well as a way we try to translate that for small to medium businesses.

Mr. LIPINSKI. Thank you. I wanted to follow up on that. Looking more generally at both for cybersecurity education and manufacturing, in 2018 the Administration put out the Strategy for American Leadership in Advanced Manufacturing. This was the result of a bill that I had written, that this Committee had passed, and it was passed into law. And so it—that strategy talks specifically about bolstering cybersecurity education and manufacturing.

So in response, the Department of Defense launched a National Center for Cybersecurity Manufacturing in 2018 at MxD (Manufacturing times Digital), which is in Chicago. The center focuses on ensuring small- and medium-size manufacturers are taking the necessary precautions to protect themselves from cyber attacks and subsequent data breaches and IP (Internet Protocol) theft.

So, Mr. Petersen, I wanted to ask, as you've discussed in your testimony the National Initiative for Cybersecurity Education is beginning the process of updating their 5-year strategic plan, so how will the framework leverage work done in manufacturing institutes like the cybersecurity center at MxD to accelerate and enhance NIST cybersecurity workforce development?

Mr. PETERSEN. So one of the roles that NICE plays is being aware of the ecosystem that's happening across the United States, not only geographically but by critical infrastructure sectors. There are other economic sectors. And NIST also, as you know, is home to the Manufacturing Extension Partnership that helps to administer some of the manufacturing programs across the United States.

And so, fortunately, in the context of my relationship with the NIST MEP (Manufacturing Extension Partnership) office, they brought the workforce program of MxD to our attention, and we have engaged with them directly. Primarily, as they go down a path of developing a workforce framework for manufacturing to create a skilled cybersecurity workforce to recognize that the NICE Cybersecurity Workforce Framework is a resource to them, it's a reference resource upon which all the critical infrastructure sectors can leverage and modify and adapt to meet their needs. But also we're trying to create a standardized environment across the Nation for cybersecurity work that can help education and training providers, as well as employers, to have that common taxonomy. So I'm glad to say we've worked with them very collaboratively and try and encourage them to use our existing framework as the foundation for what they do.

But second, as you indicate, both as we update our NICE framework and our next strategic plan, that any feedback or input that they have to provide to us, that we're more than happy to receive that as well. We did just complete a request for comment period and are going to be looking at the comments received as a way to collect that public input.

Mr. LIPINSKI. Thank you. And I want to thank you, Mr. Petersen, and all of our witnesses today for your testimony but also for your continued work on this very, very critical issue. I yield back.

Chairwoman STEVENS. Thank you, Dr. Lipinski. And I second your comments of gratitude. So many amazing things that we touched on in just this 90-minute period. Dr. Siraj, your statements of anyone can be in cybersecurity, anyone can solve these problems in this cross-functionality and this real place of opportunity for growth.

Obviously, a lot going on in Congress today, but this is submitted for the official record. And our record is going to remain open for a couple of weeks for additional statements from Members or questions that they might have, so those might come your way as well. And we're going to keep the conversation rolling, as well as the commitment that Congress will continue to serve as an effective steward and partner in filling our workforce needs, getting rid of the mistrust and obviously the risk that not only impacts our national security, our financial security, for individuals and our overall economy. And it's a job opportunity for us as well to promote the cybersecurity workforce.

So thank you all so much. The witnesses are now excused, and the hearing is adjourned.

[Whereupon, at 11:40 a.m., the Subcommittee was adjourned.]

○