GROWING AND DIVERSIFYING THE CYBER TALENT PIPELINE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MAY 21, 2019

Serial No. 116–22

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
37–868 PDF WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
DONALD M. PAYNE, JR., New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
XOCHITL TORRES SMALL, New Mexico
MAX ROSE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMINGS, Florida

MIKE ROGERS, Alabama
PETER T. KING, New York
MICHAEL T. MCCAUL, Texas
JOHN KATKO, New York
JOHN RATCLIFFE, Texas
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi

HOPE GOINS, *Staff Director*
CHRIS VIESON, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

CEDRIC L. RICHMOND, Louisiana, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KATHLEEN M. RICE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
BENNIE G. THOMPSON, Mississippi *(ex officio)*

JOHN KATKO, New York, *Ranking Member*
JOHN RATCLIFFE, Texas
MARK WALKER, North Carolina
VAN TAYLOR, Texas
MIKE ROGERS, Alabama *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
SARAH MOXLEY, *Minority Subcommittee Staff Director*

CONTENTS

GROWING AND DIVERSIFYING THE CYBER TALENT PIPELINE

Tuesday, May 21, 2019

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:13 p.m., in room 310, Cannon House Office Building, Hon. Cedric L. Richmond (Chairman of the subcommittee) presiding.

Present: Representatives Richmond, Langevin, Rice, Slotkin, Katko, Walker, Taylor, and Rogers (ex officio).

Mr. RICHMOND. I am going to go ahead and gavel us in so that we can give our opening statements, and hopefully, we can get through some of the testimony while we are here. But we are going to have to break for votes, which will be called anywhere probably in the next 15 minutes, and so then we will break, we will go vote, and then we will try to rush back as quickly as possible to be respectful of your time, because we are certainly glad that you are here.

So I will start off, and then I will turn it over to Ranking Member Katko.

Let me just start by staying good afternoon. I want to welcome the panelists to today's hearing on Growing and Diversifying the Cyber Talent Pipeline.

When I became Ranking Member of this subcommittee in 2015, researchers were projecting that the shortage of cybersecurity professionals would reach 1.5 million by 2020. In 2018, that research showed a current day shortage of nearly 3 million unfilled positions around the world, and over 300,000 in the United States alone.

That means that nearly one—nearly a third of the U.S. cybersecurity work force is, at this point, an empty desk.

Nevertheless, every day we introduce newer, smarter, more connected devices and infrastructure to make our lives easier, our businesses more profitable, and countless other goals. Every day, we learn new ways these devices can be hacked, disrupted, or manipulated to cause everything from minor inconveniences to major global havoc.

We have seen ransomware attacks take out entire branches of local government. We have had our personal data, intellectual property, and military secrets stolen by high-style foreign govern-

ments. It has never been more clear, we need more people at the table who know cybersecurity.

We must do more than admire the problem. This subcommittee held 3 cyber work force hearings last Congress, and learned something in all of them. Now that I have the gavel, I want to use it to drive home an important point: Diversity is essential for National security and for cybersecurity. We need to bring people to the table who have different perspectives, different experiences, and different ways of looking at a problem. Right now the vast majority of cybersecurity work force is white and male. Only 9 percent are African American, 4 percent are Hispanic, and 11 percent are women.

My concern is that having such a homogenous work force could lead to blind spots, and potentially intelligence failures, particularly for Federal agencies like the Department of Homeland Security.

I know we have some panelists here today that can speak to these issues directly, and I look forward to hearing your perspectives.

Despite the good work being done in the public and private sector on cyber work force, here is what I know for sure. We still are not tapping into diverse talent streams. If we are serious about fixing this problem, we need to put our money where our mouth is. We have to stop starving the Federal programs that support cyber talent, such as the National Science Foundation, CyberCorps Scholarship for Service, whose budget is on the chopping block every year.

We also need to stop bleeding talent at the very agencies who need cyber experts to carry out their missions, like DHS, the FBI, and the National Security Council at the White House. Finally, we have to move the conversation around diversity out of the background and put it in the front and center. We cannot continue to make diversity an afterthought and expect that it will spring forth naturally.

A few weeks ago, the White House issued an Executive Order on America's cybersecurity work force. It introduced a President's Cup Cyber Competition, and some work force rotation opportunities, which are good, but was mostly silent on diversity.

Officials reportedly explained that they hoped diversity would be a natural byproduct of the order. That is exactly the type of thinking we cannot afford to have if we are serious about reversing trends.

[The statement of Chairman Richmond follows:]

STATEMENT OF CHAIRMAN CEDRIC L. RICHMOND

MAY 21, 2019

When I became the Ranking Member of this subcommittee in 2015, researchers were projecting that the shortage of cybersecurity professionals would reach 1.5 million by 2020. In 2018, that research showed a current-day shortage of nearly 3 million unfilled positions around the world—and over 300,000 in the United States alone. That means that nearly a third of the U.S. cybersecurity workforce is, at this point, an empty desk. Nevertheless, every day, we introduce newer, smarter, more connected devices and infrastructure to make our lives easier, our businesses more profitable, and countless other goals. And, every day, we learn new ways these de-

vices can be hacked, disrupted, or manipulated to cause everything from minor inconveniences to major global havoc.

We have seen ransomware attacks take out entire branches of local government. We have had our personal data, intellectual property, and military secrets stolen by hostile foreign governments. It has never been more clear: We need more people at the table who know cybersecurity. And we must do more than admire the problem. This subcommittee held 3 cyber workforce hearings last Congress, and learned something in all of them. Now that I have the gavel, I want to use it to drive home an important point: Diversity is essential for National security, and for cybersecurity. We need to bring people to the table who have different perspectives, different experiences, and different ways of looking at a problem.

Right now, the vast majority of the cybersecurity workforce is white and male—only 9 percent are African American, 4 percent are Hispanic, and 11 percent are women. My concern is that having such a homogenous workforce could lead to blind spots and, potentially, intelligence failures—particularly for Federal agencies like the Department of Homeland Security. I know we have some panelists here today that can speak to these issues directly, and I look forward to their perspectives. Despite the good work being done in the public and private sector on cyber workforce, here's what I know for sure—we still are not tapping into diverse talent streams. If we are serious about fixing this problem, we need to put our money where our mouth is.

We have to stop starving the Federal programs that support cyber talent, such as the National Science Foundation's Cyber Corps Scholarship for Service, who's budget is on the chopping block every year. We also need to stop bleeding talent at the very agencies who need cyber experts to carry out their missions, like DHS, the FBI, and the National Security Council at the White House. And finally, we have to move the conversation around diversity out of the background and put it front-and-center. We cannot continue to make diversity an afterthought and expect that it will spring forth naturally.

A few weeks ago, the White House issued an Executive Order on America's Cybersecurity Workforce. It introduced a President's Cup Cyber Competition, and some workforce rotation opportunities—which are good—but was mostly silent on diversity. Officials reportedly explained that they "hoped diversity would be a natural by-product" of the Order. This is exactly the type of thinking we cannot afford to have if we are serious about reversing trends. I look forward to hearing from our witnesses today about opportunities to address this important National security issue.

Mr. RICHMOND. I look forward to hearing from our witnesses today about opportunities to address this important National security issue. With that, I will yield to the Ranking Member, Mr. Katko.

Mr. KATKO. Thank you, Mr. Chairman, for today's hearing on the cybersecurity work force.

As I meet with those involved in cybersecurity, the common refrain from Government, academia, and industry, is a need for more people. As the Chairman said, there is about 300,000 open positions in the cybersecurity field in the United States right now.

How do we fix this? To start, we much begin engaging students in primary and secondary school. We can't wait until college to introduce cybersecurity as a profession.

To that, we need more teachers that are cyber aware and curriculums that help inspire and encourage kids to engage with cybersecurity. For those that want to go to college, we need to make sure the programs are building the experience and knowledge that employers need. We also need to make sure we have professors to do that.

I am heartened that in my district, Le Moyne College is starting up a cybersecurity program this year. But it is—you know, we need a lot more than just one school doing that.

Enabling programs that grant a range of students the opportunity to engage in cybersecurity scholarship should be a top priority. I recently discussed cybersecurity scholarship opportunities

offered by the National Science Foundation through their CyberCorps program. By offering prospective students the opportunities to develop the critical skills in exchange for Government service, we ensure that we have highly-skilled cybersecurity employees in the Government, while creating the next generation of cybersecurity experts.

College is not the only pathway to a career in cyber. We need to not only develop and scale programs, but also need to increase the awareness of them. We need to provide opportunities to reskill those currently in the work force who are interested in moving to a career in cyber.

We must do more in the short term as well. I had the opportunity to talk with employees at the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency yesterday, or CISA, and the common theme among them was the challenges in hiring, and then retaining skilled employees after they train them up.

It is critical that we do more now that give CISA the tools that they need to more quickly bring on qualified personnel, particularly to join the Hunt and Incident Response Team, or HIRT, and the National Cybersecurity Assessment and Technical Security Lab, or NCATS.

The men and women in these offices are working around the clock to identify and mitigate cyber vulnerabilities in both the Government domain, and on behalf of the private sector, and they are expanding every day in those efforts.

Over the past few years, Congress has given CISA significant new authorities to harden our cyber defenses, but we have to cut the red tape so we can hire faster and keep that personnel longer.

There is no silver bullet to solve the problem, and the Federal Government cannot go it alone. It will take time. It will take effort. It will take more ideas and collaboration.

I look forward to working with my colleagues on both sides of the aisle to make a dent in the cyber work force shortage.

Thank you to our witnesses for speaking with us today.

Mr. Chairman, I yield back the balance of my time.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

MAY 21, 2019

As I meet with those involved in cybersecurity, the common refrain from Government, academia, and industry is the need for more people.

Despite having the best and the brightest students and professionals in the world, the United States still has 300,000 open positions in the cybersecurity field.

How do we fix this? To start, we must begin engaging students in primary and secondary school. We cannot wait until college to introduce cybersecurity as a career profession.

To do that, we need more teachers that are cyber aware and curriculums that help inspire and encourage kids to engage with cybersecurity.

For those that want to go to college, we need to make sure the programs are building the experience and knowledge that employers need. We also need to make sure we have professors to do that.

Enabling programs that grant a range of students the opportunity to engage in cybersecurity scholarship should be a top priority. I recently discussed cybersecurity scholarship opportunities offered by the National Science Foundation through their CyberCorps program. By offering prospective students the opportunity to develop the critical skills in exchange for Government service, we insure that we have high-

ly-skilled cybersecurity employees in the Government while creating the next generation of cybersecurity experts.

College is not the only pathway to a career in cyber. We need to not only develop and scale programs, but also increase the awareness of them.

We need to provide opportunities to reskill those currently in the workforce who are interested in moving to a career in cyber.

We must do more in the short term as well. I had the opportunity to talk with employees at the DHS Cybersecurity and Infrastructure Security Agency yesterday and a common theme was challenges in hiring and retaining skilled employees.

It is critical that we do more now to give CISA the tools to more quickly bring on qualified personnel, particularly to join the Hunt and Incident Response Team (HIRT) and the National Cybersecurity Assessments and Technical Security (NCATS) Lab.

The men and women in these offices are working around the clock to identify and mitigate cyber vulnerabilities in both the .gov domain and on behalf of the private sector. Over the past few years, Congress has given CISA significant new authorities to harden our cyber defenses but we have to cut the red tape so they can hire faster and keep their personnel.

There is no silver bullet to solve the problem. And the Federal Government cannot go it alone. It will take time, effort, new ideas and collaboration.

I look forward to working with my colleagues to make a dent in the cyber workforce shortage.

Mr. RICHMOND. I want to thank the Ranking Member, Mr. Katko from New York, for his opening statement and remind Members that other Members of the subcommittee are reminded that under the committee rules, opening statements may be submitted for the record.

[The statements of Chairman Thompson and Honorable Jackson Lee follow:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

MAY 21, 2019

Good afternoon. I want to thank Chairman Richmond for holding today's hearing on an issue critical to both our National security and our economy: Addressing the cybersecurity workforce shortage.

Today, North America's cybersecurity workforce is nearly a half-million people short—globally, the delta is nearly 3 million.

On a bipartisan basis, this committee has devoted considerable time to understanding potential consequences of the cybersecurity workforce shortage, its root causes, and how the Federal Government can most effectively partner with the private sector to develop cyber talent.

The White House reported last year that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Those figures have almost certainly grown since.

We also know that sophisticated foreign adversaries are constantly seeking novel ways to attack our critical infrastructure and steal sensitive National security information.

So, it is clear that failing to grow the cyber talent pipeline could have catastrophic consequences.

As we have worked to better understand the roots or our cybersecurity workforce shortage, one thing has become clear: We aren't looking for talent in the right places and, as a result, our Federal policies are not effectively targeting untapped talent pools.

(ISC)2 and the International Consortium of Minority Cybersecurity Professionals conducted a survey last year that revealed African Americans make up only 9 percent of the cybersecurity workforce and Hispanics comprise only 4 percent.

Women are similarly underrepresented.

Over time, we have learned that our workforce shortages stem—in part—from misconceptions about the education levels required to work in cybersecurity.

Not all cybersecurity positions require 4-year degrees, and we need to do a better job making sure the public understands that.

At the same time, women and minority groups holding cybersecurity jobs tend to have higher education levels but are less likely to hold management positions or receive salary increases.

That brings me to another observation: The cybersecurity field has struggled to adapt to the demands of diversity, including being slow to create opportunities for training and advancement for diverse candidates.

That is why I am pleased that we have a diverse set of panelists with a range of experience here today to help us better understand how we can bring more people into the cybersecurity field.

We need to have a soup-to-nuts conversation about how to attract new people from different backgrounds to cybersecurity jobs, and then retain them.

Growing and diversifying the cyber talent pipeline will require the Federal Government to improve that way it partners with the private sector and the public to achieve three objectives:

- First, we must cultivate an interest in cybersecurity careers in diverse communities;
- Second, we must connect people with educational and training opportunities;
- Finally, we must provide a bridge between training and careers.

The Federal Government's current workforce initiatives start to address some, but not all, of these objectives.

For example, the Department of Homeland Security and the National Science Foundation provide scholarships and stipends to students seeking cybersecurity-related degrees, and DHS also works with the National Security Agency to support the designation of over 200 colleges and universities as either National Centers of Academic Excellence.

And NIST developed the NICE National Cybersecurity Workforce Framework to match job descriptions with job seekers.

But I am not certain that any of these well-intentioned initiatives successfully attract new people to the field.

Even the Executive Order on the Cybersecurity Workforce signed earlier this month is largely silent on diversity.

Indeed, the EO could actually create barriers to growing the cyber talent pool by implementing "aptitude assessments" for agencies to use when identifying employees to reskill for cybersecurity.

To fill gaps in the Federal Government's cybersecurity workforce policy, we need to hear from diverse voices like those before us today.

With that, I thank the witnesses for being here today and look forward to our discussion.

I yield back the balance of my time.

STATEMENT OF HONORABLE SHEILA JACKSON LEE

MAY 21, 2019

Chairman Richmond and Ranking Member Katko, thank you for holding today's hearing on "Growing and Diversifying the Cyber Talent Pipeline."

This hearing provides Members an opportunity to learn about the current shortage of skilled cybersecurity professionals, the lack of diversity in the field, and academic initiatives to address workforce challenges.

The Federal Government, including the Department of Homeland Security (DHS), can support efforts to grow and diversify the cyber talent, and leverage these talent streams to recruit and retain cyber experts in civil service.

I look forward to the testimony of today's witnesses:

- Wesley Simpson, chief operating officer, International Information System Security Certification Consortium ((ISC)^2);
- Richard "Rick" Gallot, president, Grambling State University;
- Dr. Amelia Estwick, National Cybersecurity Institute, Excelsior College; and
- Candace Worley, vice president and chief technical strategist, McAfee (Minority witness).

The cybersecurity field's has an expanding shortage of professionals, with over a quarter-million positions remaining unfilled in the United States alone and a predicted shortfall of 1.5 million cybersecurity professionals by 2019.

The solution must be to grow a greater pool of cybersecurity professionals that are prepared to fill positions within the Federal Government.

The strength of the U.S. cybersecurity workforce is paramount to our National security and economic stability, but there are 300,000 unfilled positions in the United States, and close to 3 million world-wide.

Congress must intervene to stop this gap from widening.

The challenge before the Homeland Security Committee is finding the right policy that will accomplish the goal of attracting and retaining cybersecurity professionals within the Federal Government.

I have focused on this problem and have mapped out a comprehensive approach to meeting the underlying problem: Increasing the pool of people who would receive essential education in science, technology, engineering, and mathematics from kindergarten through advanced degree programs.

In 2017, I was pleased to have been awarded the Executive Women's Forum's Women in Cybersecurity Leadership Award for my work in promoting advances in our cybersecurity policy.

I participated on a leading cybersecurity panel at the 2018 Aspen Institute Cyber Summit in San Francisco.

The Trump administration's new Executive Order on America's Cybersecurity Workforce does not do enough to grow the cybersecurity talent pipeline and could unnecessarily exclude qualified candidates by relying on aptitude assessments, which tend to yield biased outcomes.

Committee Democrats will push the White House to fully leverage Federal resources to grow and diversify that cybersecurity talent pipeline.

I was pleased to attend the Aspen Institute to discuss the role of Government in creating a policy and framework for our Nation which will protect Government and civilian computer networks by current and future threats, such as quantum computing, advances in artificial intelligence, and unknown—but likely and anticipated—threats posed from future technological innovations on the horizon.

The beginning of the Government's ability to protect networks and computing technology begins with the talent we can attract to the Department of Homeland Security.

In our pursuit of closing the gap between minority and majority participation in cybersecurity, we must also look at promotion and retention issues as well.

The (ISC)[2] Global Information Security Workforce Study that covered the period from June 22 through September 11, 2016, and features a deeper dive into the diverse composition of the U.S. cybersecurity workforce to encompass not only gender, age, and tenure, but ethnicity and race as well.

Among minority cybersecurity professionals, 23 percent hold a role of director or above, 7 percent below the United States average.

They found that minorities who have advanced into leadership roles often hold higher degrees of academic education than their Caucasian peers who occupy similar positions; of minorities in cybersecurity, 62 percent have obtained a master's degree or higher, compared to 50 percent of professionals who identified as White or Caucasian.

The 2017 Global Information Security Workforce Study examined both conscious and unconscious forms of discrimination in the workplace.

They considered unfair treatment based on gender, age, ethnicity, or an employee's cultural group.

The survey found discrimination based on ethnicity and gender.

Thirty-two percent of cybersecurity professionals of color who participated in the survey report that they have experienced some form of discrimination in the workplace.

Across all races and ethnicities, women experience greater rates of discrimination in the workplace than men, reporting discrimination in much greater proportions than men when viewed as a total U.S. population.

Women who identify as Black, Hispanic, Asian, or of Native American descent, report the highest numbers of discrimination.

CONGRESSWOMAN JACKSON LEE'S LEGISLATIVE EFFORTS TO CLOSE THE CYBERSECURITY WORKFORCE GAP

I will soon be reintroducing the Cyber Security Education and the Workforce Enhancement Act, which seeks to prepare more women and minority students and early stage to mid-career professionals within the Federal Government for cybersecurity jobs.

The bill supports:

- Recruiting information assurance, cybersecurity, and computer security professionals;
- Providing grants, training programs, and other support for kindergarten through grade 12, secondary, and post-secondary computer security education programs;
- Supporting guest lecturer programs in which professional computer security experts lecture computer science students at institutions of higher education;

- Identifying youth training programs for students to work in part-time or summer positions at Federal agencies; and
- Developing programs to support underrepresented minorities in computer security fields with programs at minority-serving institutions, including Historically Black Colleges and Universities, Hispanic-serving institutions, Native American colleges, Asian-American institutions, and rural colleges and universities.

The goal of the Cyber Security Education and the Workforce Enhancement Act is to address underrepresentation of women and minorities in cybersecurity fields of employment.

CYBERSECURITY STATISTICS

In 2016, the Bureau of Labor Statistics reported that African-Americans comprised only 3 percent of the information security analysts in the United States, yet comprise nearly 13 percent of the National population.

Just 2 years ago a security analyst, a position which required a 4-year degree, was paid on average $88,890 per year.

The top computing security salaries range from $175,000 to $230,00 per year.

The most senior position was chief information security officers (CISOs), which typically earns $400,000 or more per year.

In 2017 the United States employed nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity employment vacancies.

In 2017, nearly 65 percent of large U.S. companies have a chief information security officer, up from 50 percent in 2016.

Women hold only 11 percent of cybersecurity positions globally, while filling 25 percent of tech jobs, and comprising 50 percent of the population.

During this time of the year, I speak at commencement exercises and given these statistics my message to young people is to look to the cybersecurity field for career and employment opportunities.

There is a similar situation with African Americans which comprise only 7 percent of the cybersecurity workforce, and Hispanics, who account for 5 percent of cybersecurity positions although they make up 13 percent of the Nation's population.

Finally, 2 out of 3 high school students indicate that no one has ever spoken to them about a career in cybersecurity.

These facts mean that we should not have any shortages for computing security jobs, but that these vacancies exist because of barriers to entry like education.

SOLUTION FOR EXPANDING THE FEDERAL CYBERSECURITY WORKFORCE

The solution is expanding the diversity of those who are cybersecurity professionals by tapping human capital already within the Federal Government in new hires or mid-career changes, when we identify that someone has the aptitude and desire to become a computing security professional.

AFRICAN AMERICAN PIONEERS IN COMPUTER SCIENCE

Katherine G. Johnson, of Hidden Figures fame, graduated from college at age 18. In 1952, she began working at NASA in its aeronautics area as a "computer," where she performed the calculations that assured that when astronauts were sent into orbit they could be safely returned to earth.

Roy Clay Sr. is known as the Godfather of Silicon Valley. Mr. Clay was at the cutting edge of computing and technology through his leadership of HP's first foray into the computer market with its 2116A computer.

He was inducted into Silicon Valley Engineering Council's Hall of Fame in 2003.

Mark Dean co-created the IBM personal computer and was instrumental in the development of the company's PC 5150, which was sold to the public in 1981.

Mr. Dean also contributed to the development of the color PC monitor, the first gigahertz chip, and the industry standard architecture (ISA) system bus.

The personal computers' impact on our world is unmistakable.

In the early days of the computing technology age, computers were only available to governments and large institutional organizations because of their size and complexity.

The age of personal computing has paved the way for mobile computing and handheld computing devices like smart phones.

WOMEN AND THE HISTORY OF COMPUTING

Augusta Ada King-Noel, Countess of Lovelace was an English mathematician and writer, chiefly known for her work on Charles Babbage's proposed mechanical general-purpose computer.

She was the first to recognize that the machine had applications beyond pure calculation, and created the first computer program to give Babbage's machine instructions to carry out a task.

As a result, she is often regarded as the first to recognize the full potential of a "computing machine," and the first computer programmer.

Grace Hopper was an American computer scientist and United States Navy rear admiral, who became the first programmer of the Harvard Mark I computer and she invented the first compiler for a computer programming language.

The Executive Women's Forum (EWF) recognizes the contributions women have made and seeks to expand opportunities for women.

The Executive Women's Forum was founded in 2002, with a mission of inspiring leaders, transforming organizations and building businesses through education, leadership development and the creation of trusted relationships.

Today, the EWF has over a thousand members Nation-wide—from emerging leaders to senior executives, all of whom benefit from the organization's programs and events.

EWF members support each other in achieving their goals and advancing their careers by celebrating each other's accomplishments and acknowledging the ideas and contributions of the women around us.

Most notably, each year EWF presents Women of Influence Awards to individuals who have made outstanding contributions in the corporate, Government/academic and vendor sectors.

The EWF's, "2017 Global Information Security Workforce Study: Women in Cybersecurity" report delivers troubling statistics on areas we are missing the mark in maximizing the participation of women in the cybersecurity workforce.

Fifty-one percent of women report various forms of discrimination in the cybersecurity workforce.

Women who feel valued in the workplace have also benefited from leadership development programs in greater numbers than women who feel undervalued.

In 2016 women in cybersecurity earned less than men at every level.

We know that cybersecurity expertise is a critical component of National security; however, Federal agencies have traditionally struggled to recruit, retain, and manage a robust cybersecurity workforce.

The International Consortium of Minority Cybersecurity Professionals (IC–MCP) launched in 2014 with a mission to bridge this "great cyber divide" in the cybersecurity profession. ICMCP offers programs and services to these groups to assist them in gaining skills and visibility to promote their careers, including:

- Mentoring opportunities for entry- and mid-career cybersecurity professionals;
- Networking opportunities;
- Skills workshops.

In 2015, I was pleased to host the International Consortium of Minority Cybersecurity Professionals for its first meeting held on Capitol Hill.

The vision of ICMCP is to build a pipeline of cybersecurity professionals at all levels, and support them throughout their careers.

ICMCP efforts have the potential to broaden the pool of available experienced cybersecurity professionals.

This Congress I introduced H.R. 1981, the Cyber Security Education and Federal Workforce Enhancement Act, which creates programs to support underrepresented minorities in computer security fields.

I understand that the supply of educated and certified cybersecurity professionals is too few when compared with the thousands of positions that need them.

As a result, talented candidates can demand higher salaries, more flexible hours, and other benefits that are incompatible with the Federal hiring process.

Priorities within the workforce have also changed.

For instance, millennials change employers more frequently than their predecessors and place a high value on flexible work schedules and professional development opportunities.

I strongly believe that we have untapped talent within the Federal workforce, and we have potential pools of talented young people who are in underrepresented communities around the Nation that we must reach during their formative education to prepare them for potential cybersecurity careers.

We are not supporting DHS with a policy that would allow the agency to pursue talent regardless of where it might be found.

So long as DHS attempts to compete for cybersecurity talent in the same market where the private-sector businesses are competing, the results will not change.

We must be creative and engage in broader thinking that does not limit our view of who can be a cybersecurity professional.

POTENTIAL FOR DHS TO SUCCEED IN RECRUITMENT AND RETENTION OF CYBERSECURITY PROFESSIONALS

The 2017 Global Information Security Workforce Study: Women in Cybersecurity issued by the Executive Women's Forum, stresses what we already know; some segments of the workforce are underrepresented in the cybersecurity field. Women professionals make up only 11 percent of the cybersecurity workforce despite the escalating growth in the field.

The participation of women in cybersecurity is at 11 percent although women reported higher levels of education.

These underrepresented groups offer an opportunity to increase the cybersecurity workforce in the near and long term.

This is important because both Gen Y and Gen Z have significant numbers of minorities who could significantly close the cybersecurity gap.

I look forward to working with the Chair and Ranking Members on increasing diversity in the Federal cybersecurity workforce.

Thank you.

Mr. RICHMOND. I now want to welcome our panel of witnesses.

First, we have Mr. Wesley Simpson, the chief operating officer for the International Information Systems Security Certification Consortium, better known as (ISC)².

(ISC)² is the world's largest IT security organization for cybersecurity professionals, and we rely heavily on the studies they produce, and the data they use to track work force trends in the United States and abroad. I had the pleasure of speaking at their conference last year in New Orleans.

Next, I would like to welcome my friend, former colleague in the Louisiana State House, former State senator, and president Rick Gallot of Grambling State University, an HBCU in Louisiana that produces 40 percent of the State's African American computer science graduates, and plans to begin offering a new bachelor's degree in cybersecurity this year.

I hope you will tell us how we can build better partnerships to help the Federal Government leverage the talent coming out of minority-serving institutions like Grambling State University.

We also have Dr. Amelia Estwick from the National Cybersecurity Institute at the Excelsior College.

Dr. Estwick has spent her career on the front lines of this issue; first in the United States Army, then for 15 years at the National Security Agency, where she was a technical director for cyber threat operations.

I look forward to hearing her unique perspective as a veteran, a former Federal official, and in academia, where she is helping to educate the next generation of cybersecurity professionals.

Finally, I would like to welcome Ms. Candace Worley, the vice president and chief technical strategist for McAfee, who will tell us about some of the good work being done in the private sector to grow and diversify this cyber talent pipeline.

Mr. RICHMOND. Without objection, the witnesses' full statements will be inserted into the record. I will now ask each witness to summarize his or her statement in 5 minutes, beginning with Mr. Simpson.

STATEMENT OF WESLEY SIMPSON, CHIEF OPERATING OFFICER, INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM

Mr. SIMPSON. Mr. Chairman and esteemed Members of the committee, thank you for inviting me here today to testify on behalf of (ISC)² regarding the goal of a more inclusive and diverse cybersecurity work force.

My name is Wesley Simpson, and I am the chief operating officer for (ISC)², headquartered in the United States.

(ISC)² is the world's largest nonprofit membership association of certified cybersecurity professionals. We function as an advocate for the cybersecurity profession, and as a training and certification body.

Our certifications are approved by the American National Standards Institute, or ANSI, which the primary organization for fostering the development of technology standards in the United States.

As part of our association's stated mission to inspire a safe and secure cyber world, we regularly commission market research and a host of relevant industry topics that help to inform our global base of more than 140,000 certified members across more than 170 countries, as well as influence policy discussions, corporate programs, and educational opportunities.

In the course of doing so, we have issued research related to the size of the cybersecurity work force gap since 2004. The state of the industry has changed quite a bit over that time, and (ISC)² is constantly identifying ways to improve its research methodology to keep up with the evolution of the marketplace.

As part and parcel of the work force research, we are in position to be able to identify the demographic makeup of the cybersecurity work force as it changes, and I am pleased to share some of those findings with you today, as well as some conclusions we might draw from them.

A recent round of work force research was conducted in 2018, and it reveals a cybersecurity work force shortage of 498,000 skilled professionals just in the United States, and 2.93 million globally. This points to a growing gap in the amount of cybersecurity staff the private sector and governing bodies indicate they need to maintain optimal security, and the amount of skilled professionals currently available.

As a point of clarification, this is not meant to indicate that there are currently one-half open—million open or unfilled jobs.

As we collectively explore ways in which the talent pool can be increased, it is important to recognize the clear underrepresentation of women in the cybersecurity work force.

While Department of Labor statistics indicate that women make up 47 percent of the overall U.S. labor force, our research shows that only constitutes 22 percent of U.S. cybersecurity staff, and only 24 percent of the global staff.

To be more specific, that figure includes anyone from whom at least 20 percent of their daily job tasks consists of security-related activities, not just those with cybersecurity titles. This expands our view to include those with IT roles, for example, who have some cybersecurity responsibilities. This change to our methodology was

made in 2018 to more closely mirror the reality of how cybersecurity is executed around the ground levels, and, more importantly, by who.

We also found that pay and equity between genders remains an issue, and is something that could affect a woman's decision to pursue a career in this field.

If we can find ways to attract women to cybersecurity and make it a welcoming profession, we may be able to decrease the cybersecurity work force gap to a large degree. There are more findings specific to our 2019 "Women in Cybersecurity" report found in my written testimony. But I want to highlight the obvious underrepresentation as a key datapoint for our discussion here today.

Another underrepresented group identified through our research is ethnic and racial minorities. Our 2018 study titled "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," showed that just 26 percent of the U.S. cybersecurity work force identifies as non-Caucasian. While this compares favorably with the Department of Labor statistics that shows only 22 percent of the overall U.S. labor force is made up of minorities, this is still a low ratio that could be improved by creating programs that specifically market the path to a cybersecurity career to a wider talent pool.

Furthermore, employment among cybersecurity professionals who identify as racial or ethnic minorities tends to be concentrated in nonmanagement positions, with fewer occupying leadership roles, despite being highly educated. Here as well, our research showed that inequity in pay exists. Despite higher levels of education, a cybersecurity professional of color earns less than their Caucasian counterparts, on average.

Under-participation in cybersecurity by large segments of our potential work force, be it women or minorities, represents a loss of opportunities for individuals, and a loss of collective creativity in solving the problems we face in the field. Not only is this an issue of inequity, it is a threat to our global economic viability as a Nation.

The major opportunities, as we see them, are stronger, more focused on equal pay for women and minorities in cybersecurity, more advancement and leadership opportunities for deserving professionals, formalized mentorship programs to help unearth untapped potential and hidden talent, and more programs that expose young women and minorities to technical skills earlier in their educational lives.

I thank you for your time today, and look forward to answering any questions you may have to the best of my ability.

[The prepared statement of Mr. Simpson follows:]

PREPARED STATEMENT OF WESLEY SIMPSON

MAY 21, 2019

Mr. Chairman and esteemed Members of the committee, thank you for inviting me here today to testify on behalf of (ISC)² regarding the goal of a more inclusive and diverse cybersecurity workforce. My name is Wesley Simpson, and I am the chief operating officer for (ISC)². Headquartered right here in the United States, (ISC)² is the world's largest nonprofit membership association of certified cybersecurity professionals. We function as an advocate for the cybersecurity profession and as a training and certification body. Our certifications are approved by the American

National Standards Institute (ANSI), which is the primary organization for fostering the development of technology standards in the United States.

As part of our association's stated mission to inspire a safe and secure cyber world, we regularly commission market research on a host of relevant industry topics that help to inform our global base of more than 140,000 certified members across more than 170 countries, as well as influence policy discussions, corporate programs, and educational opportunities. In the course of doing so, we have issued research related to the size of the cybersecurity "workforce gap" since 2004. The state of the industry has changed quite a bit over that time, and (ISC)[2] is constantly identifying ways to improve its research methodology to keep up with the evolution of the market.

As part and parcel of our workforce research, we are in a position to be able to identify the demographic make-up of the cybersecurity workforce as it changes, and I'm pleased to share some of those findings with you today, as well as some conclusions we might draw from them.

Our most recent round of workforce research was conducted in 2018 and reveals a cybersecurity workforce shortage of 498,000 skilled professionals in the United States alone, and 2.93 million globally. This points to a growing gap in the amount of cybersecurity staff that private sector and Government bodies indicate they need to maintain optimal security, and the amount of skilled professionals currently available. As a point of clarification, this is not meant to indicate that there are currently one-half million open or unfilled jobs.

As we collectively explore ways in which the talent pool can be increased, it's important to recognize the clear under-representation of women in the cybersecurity workforce. While Department of Labor statistics [1] indicate that women make up 47 percent of the overall U.S. labor force, our research shows that they only constitute 22 percent of U.S. cybersecurity staff, and only 24 percent of global staff. To be more specific, that figure includes anyone for whom at least 25 percent of their daily job tasks consist of security-related activities, not just those with cybersecurity titles. This expands our view to include those with IT roles, for example, who have some cybersecurity responsibilities. This change to our methodology was made in 2018 to more closely mirror the reality of how cybersecurity is executed at the ground level, and more importantly, by who. We also found that pay inequality between genders remains an issue and is something that could affect a woman's decision to pursue a career in our field.

If we can find more ways to attract women to cybersecurity and make it a welcoming profession, we may be able to decrease the cybersecurity workforce gap to a large degree. There are more findings specific to our "2019 Women in Cybersecurity Report" found in my written testimony, but I wanted to highlight the obvious underrepresentation as the key data point for discussion here today.

Another underrepresented group identified through our research is ethnic and racial minorities. Our 2018 study titled, "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," showed that just 26 percent of the U.S. cybersecurity workforce identifies as non-Caucasian. While this compares favorably to Department of Labor statistics that show only 22 percent of the overall U.S. labor force is made up of minorities,[2] this is still a low ratio that could be improved by creating programs that specifically market the path to a cybersecurity career to a wider talent pool.

Furthermore, employment among cybersecurity professionals who identify as racial or ethnic minorities tends to be concentrated in non-management positions, with fewer occupying leadership roles, despite being highly educated. And here as well, our research showed that an inequity in pay exists. Despite higher levels of education, a cybersecurity professional of color earns less than their Caucasian counterparts on average.

Under-participation in cybersecurity by large segments of our potential workforce, be it women or minorities, represents a loss of opportunity for individuals and a loss of collective creativity in solving the problems we face in the field. Not only is this an issue of inequity, it is a threat to our global economic viability as a Nation. The major opportunities as we see them are a stronger focus on equal pay for women and minorities in cybersecurity, more advancement and leadership opportunities for deserving professionals, formalized mentorship programs to help unearth untapped potential and hidden talents, and more programs that expose young women and minorities to technical skills earlier in their educational lives.

---

[1] U.S. Department of Labor—*https://www.dol.gov/wb/stats/NEWSTATS/latest/demographics.htm#LF-SecRaceEthnicity*.

[2] U.S. Department of Labor—*https://www.bls.gov/opub/reports/race-and-ethnicity/2017/home.htm*.

I thank you for your time today and look forward to answering any questions you may have to the best of my ability.

Following are key data points from (ISC)²'s two most recent studies that touch on diversity. The first is the "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce" study (submitted as Exhibit A) which was released in March 2018 (based on 2017 data from the (ISC)² Global Information Security Workforce Study—submitted as Exhibit B). The second is the "2019 Women in Cybersecurity Report" (submitted as Exhibit D) (sourced from data within the 2018 Cybersecurity Workforce Study—submitted as Exhibit C). Key data points from each are identified below.

MINORITIES IN CYBERSECURITY

The diversity report was developed by (ISC)² and The Center for Cyber Safety and Education in partnership with Frost & Sullivan. Although the study is global in its scope, questions of race and ethnicity were asked only to respondents in the United States. This report was developed by (ISC)² in partnership with the International Consortium of Minority Cybersecurity Professionals (ICMCP). Findings were based on survey responses from 9,500 U.S. cybersecurity professionals.

Employment among cybersecurity professionals who identify as a racial or ethnic minority tends to be concentrated in non-management positions, with fewer occupying leadership roles, despite being highly educated.

Key Findings

- Minority representation within the cybersecurity field is at 26 percent, which is slightly higher than the overall U.S. minority workforce, which was at 21 percent at the time the study was conducted.
- 62 percent of minorities in cybersecurity have obtained a master's degree or higher, compared to 50 percent of professionals who identified as White or Caucasian.
- 23 percent of minority cybersecurity professionals hold a role of director or above, compared to 30 percent of their Caucasian peers.
- On average, a cybersecurity professional of color earns $115,000, while the overall U.S. cybersecurity workforce average is $122,000.
- 32 percent of cybersecurity professionals of color report that they have experienced some form of discrimination in the workplace.
- To foster diversity in the workplace, 49 percent of minority cybersecurity professionals said mentorship programs are very important.

Conclusions

- Despite higher levels of education, a cybersecurity professional of color earns less and is underrepresented in senior roles.
  - Racial and ethnic minorities tend to hold non-managerial positions, and pay discrepancies, especially for minority women (women of color make an average of $10,000 less than Caucasian males and $6,000 less than Caucasian females), is a challenge.
- With the estimated global cybersecurity workforce shortage at 2.93 million, we need to make the profession inviting to all.
- Understanding the challenges our profession faces related to diversity is a critical first step in accomplishing that goal and ultimately addressing the widening cybersecurity workforce gap.
- Mentorship programs and better representation in senior roles are needed to help advance minority cybersecurity professionals.
- Companies with more diverse workplaces perform better financially. (Data from McKinsey and Company report titled: "Is There a Payoff from Top-Team Diversity?")

Key Takeaway

- Under-participation in cybersecurity by large segments of our potential workforce represents a loss of opportunity for individuals and a loss of creativity in solving the problems we face in the field. Not only is this an issue of inequity, it is a threat to our global economic viability as a Nation. The major opportunities as we see them are a stronger focus on equal pay for minorities in cybersecurity, more advancement and leadership opportunities for deserving professionals, and formalized mentorship programs to help unearth untapped potential and hidden talents.

WOMEN IN CYBERSECURITY

On Tuesday, April 2, 2019, (ISC)² issued its 2019 Women in Cybersecurity Report (sourced from data within the 2018 Cybersecurity Workforce Study). The headline finding from the report was that women make up an estimated 24 percent of the global cybersecurity workforce.

It's important to understand where this number came from. The figure is derived from the Workforce Study, which was actually fielded twice within the 2018 calendar year in order to confirm the relative accuracy and integrity of the data. Both waves of research produced the same statistically valid results.

Last year's global Workforce Study was a departure from the way past studies have been fielded and the way the workforce gap had been calculated previously, and that's what has led to a seeming increase of women in the field from 11 percent to 24 percent over the 2-year period since we released our last Women in Cybersecurity report. As such, we do not make the claim that there has been a 13 percent increase over a 2-year period, but we feel that our new methodology (explained in the section below) provides a more accurate picture than ever before of the true make-up of the workforce.

IMPORTANT: We did not address the issue of discrimination against women in this report, so we don't have data to share. While it is an important topic of discussion in our industry, this particular report does not address it specifically and we focused on the demographic of professionals in the workforce as opposed to the hurdles they face.

Methodology

Past (ISC)² research had estimated the percentage of women working in cybersecurity at 11 percent, but with a change to research methodology—including surveying IT/ICT professionals who spend at least 25 percent of their time on security activities—that number is now believed to be 24 percent. Results presented in the report are extracted from a study conducted by (ISC)² and Spiceworks in August 2018. The sample structure was carefully designed to obtain feedback from a diverse group of professionals working in cybersecurity roles and the survey measured various aspects of working in the cybersecurity field including workforce staffing shortages, education and skills needed to do the job, and challenges faced in the profession. One thousand four hundred fifty-two individuals from North America, Latin America, and Asia-Pacific participated in the survey. The margin of error for this research is plus or minus 3 percent at a 95 percent confidence level.

Below are the 3 key messages that rise to the surface related to the report. Following those, some notes on other relevant data points that may be of interest.

Key Findings

(1) Today's figure reflects more women in cybersecurity than previously estimated

- 24 percent of the overall cybersecurity workforce is female. Recruiting from traditionally overlooked demographics will be a huge part of closing the current global talent gap of 2.93 million. We need more women and more young talent to join us, as well as individuals who want to transfer other skills into a career in cybersecurity; and we need to show them why and how they should do so.

(2) These women are younger, highly educated and moving into leadership roles

- 45 percent of women surveyed are millennials, compared to just 33 percent of men. This will radically alter the gender balance in the cybersecurity profession in the next decade, as the Baby Boomer generation continues to retire in larger numbers.
- Women also bring higher levels of education to cybersecurity. More women (52 percent) in the survey hold a post-graduate degree than their male counterparts (44 percent).
- Women in the field are advancing to leadership positions. Higher percentages of women than men are attaining senior leadership and decision-making positions.
  - Chief Technology Officer—7 percent of women vs. 2 percent of men
  - Vice President of IT—9 percent of women vs. 5 percent of men
  - IT Director—18 percent of women vs. 14 percent of men
  - C-level/Executive—28 percent of women vs. 19 percent of men

(3) There are still challenges to face, including pay inequity

- 17 percent of women globally reported annual salaries between $50,000–$90,000, as compared to 29 percent of men, and 15 percent of women earn between $100,000–$499,999, while 20 percent of men earn at least that much.

Other key data points to be aware of:

- Women and men have pretty much the same workplace values, priorities, and aspirations. Both place a similar level of importance on salary and working close to home and use the same skills at work.
- The report indicates that men and women share a lot of the same concerns about their roles, including lack of commitment from upper management, the reputation of their organization, risk of seeing their job outsourced, lack of work/life balance, the threat of artificial intelligence (AI) reducing the need for cybersecurity workers and a lack of standardized cybersecurity terminology to effectively communicate within their organizations.

Key Takeaway

- Although we now see women making up nearly one-quarter of the cybersecurity workforce, we need more gender balance in order to strengthen our National and global cybersecurity readiness. The opportunities that exist revolve around making cybersecurity a more attractive career path for women. This could be supported by enforcement of equal pay between genders and the creation of more programs that expose young women to technical skills earlier in their educational lives.

In terms of breaking down the roles in which women participate in cybersecurity (hence the jump from 11 percent to 24 percent), it is difficult to draw any hard and fast conclusions and this is a pretty nuanced point, but I think the first attachment to this email is a good way to look at the differences. You can see that men disproportionately outnumber women in the roles of Security Specialist and Security/Compliance Officer, both of which would be considered "cybersecurity" titles that would have been included in our research prior to 2018. When you add in roles such as Help Desk Technician, IT Director, VP IT and CTO, you can see that there are a higher percentage of women. Of course, that doesn't mean there are more women than men because women still represent a 3–1 minority ratio of the overall total in the profession, but you can see how that percentage of women starts to shoot up from 11 percent to 24 percent with the inclusion of the more general IT roles. Additionally, it's important to understand that our data prior to 2018 also largely surveyed (ISC)² members as part of the sample, and our members are required to have at least 5 years of professional experience in cybersecurity in order to earn a certification. Therefore, when we opened up the survey to a broader audience and adjusted the methodology, this led to the inclusion of many other professionals who, while they have not been certified, are still doing the work of cybersecurity. That added a larger percentage of women to the overall count.

Mr. RICHMOND. Thank you, Mr. Simpson.

I now recognize Mr. Gallot to summarize his statement for 5 minutes.

STATEMENT OF RICHARD J. "RICK" GALLOT, JR., PRESIDENT, GRAMBLING STATE UNIVERSITY

Mr. GALLOT. Thank you, Chairman Richmond, Ranking Member Mr. Katko, and the distinguished Members of the Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection.

On behalf of the team at Grambling State University, the University of Louisiana system, who is represented here by Dr. Jim Henderson, system president, and historically black colleges and universities across the United States of America, we sincerely appreciate this opportunity, and coming opportunities, to collaborate.

As president of Grambling State University, I am privileged to lead a campus community that includes more than 5,200 students, and 550 staff and faculty, as well as students who represent 42 States and 27 foreign countries, to help address Louisiana and the United States' vital work force needs for the past 118 years.

Founded in 1901, our university is well-known outside of the classroom for our historic football and Coach Eddie Robinson, our world-famed Tiger marching band, and as our motto being "the place where everybody is somebody."

In contrast, it is our innovation inside the classroom that is the true foundation for our legacy. That foundation is what provides us the opportunity to share with you today.

For generations, Grambling State University has led Louisiana in equipping and building the technology work force. As I mentioned in our submitted testimony, Grambling State University has produced technology leaders since 1972, partners with America's largest technology companies on talent development with IBM, CenturyLink, Microsoft, and many others. We continue to lead Louisiana in producing African-American computer science and computer information system graduates.

We are a small but mighty force along Interstate 20, which is fastly becoming the cyber corridor of North Louisiana. Our university's record-breaking enrollment growth, increases in fiscal health and partnerships are helping create Louisiana's most educated generation in history.

That generation includes students like Jarrid Richards. Jarrid is a senior in our computer science program, who is a great example of how holistic investment in minority students produces expert talent in the fields of technology and cybersecurity.

Today, we are able to help close the widening cybersecurity job gap by supporting students like Jarrid. During his time at Grambling State, there were a few semesters where he encountered a gap, as many of our students do, between the amount of aid and his cost to attend. While Jarrid worked three jobs around campus, there were semesters when without scholarships and grants, he may not have been able to continue his education.

When Jarrid was looking for career experience, our partnership with CLECO, a local energy provider, was able to provide him his first hands-on experience with network security and preventing cyber threats.

Those investments and the mentorship of his professor, Dr. Reddy, positioned Jarrid to finish this year with multiple internship offers and early conversations about full-time opportunities when he graduates this fall.

He is just one example of how the collaboration between HBCUs and powerful partners can help companies, communities, and, most importantly, students.

I am excited to share that our Governor, Governor John Bel Edwards, our Board of Regents, our University of Louisiana system, and communities, see our power and have selected our university to offer the State's first bachelor's degree in cybersecurity.

We are honored to lead the next generation of Louisiana innovation, and are excited to join this committee's historic discussion on how we can support our country.

We thank you for this opportunity and look forward to answering any questions, Mr. Chairman, and Ranking Member. Thank you.

[The prepared statement of Mr. Gallot follows:]

STATEMENT OF RICHARD J. "RICK" GALLOT, JR.

MAY 21, 2019

Thank you to Chairman Richmond, Ranking Member Mr. Katko, and the distinguished Members of the Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection. On behalf of the team at Grambling State University, the

University of Louisiana System, and Historically Black Colleges and Universities across the United States, we sincerely appreciate this and the coming opportunities to collaborate on addressing one of America's most critical workforce development needs.

As president of Grambling State University, I am privileged to lead a campus community that includes more than 5,200 students, 550 faculty and staff, and countless North Louisiana constituents who have helped address the vital workforce needs in our State for 119 years. Founded in 1901, our University's well-known outside of the classroom for our historic and the most-winning football coach in history, Coach Eddie Robinson; our world-famed and Super Bowl-performing Tiger marching band; and being, as our motto states, "the place where everybody is somebody."

However, it's our innovation inside of the classroom that is the true foundation for our legacy and what provides the unique opportunity to share with you.

Today, I am excited to provide background on why we were chosen as home to Louisiana's first bachelor's degree in cybersecurity and how HBCUs, like Grambling State, are well-positioned to deliver the highest return on investment when developing talent in the fields of STEM, cybersecurity, and related industries.

Since 1972, Grambling State has led Louisiana in producing African American Computer Science graduates. Our former students have gone on to lead information technology (IT) and threat prevention efforts for America's leading companies. From technology providers like CenturyLink and IBM to consumer and retail giants that include Sara Lee, General Electric, and General Motors, we have a long legacy of growing the senior-level talent that helps shape American technology.

Now, that might seem odd to hear of a small school located in rural North Louisiana, but our achievement isn't uncommon if you know the story of America's HBCUs. Today, we at Grambling State lead as Louisiana's No. 1 producer of computer and information science graduates—in fact, we outpace all others in our State by at least 27 percent. Today, we are weeks from launching America's 13th Cybersecurity undergraduate program and the first in our State. Today, we are realizing growth that includes a 5-year enrollment high, a 100 percent increase in our fiscal health score, and an economic impact of more than $175 million.

In contrast, there is another impactful fact about today that exists for us and our sister HBCUs. At GSU, while we have a long legacy of partnering with America's technology giants to grow IT innovators, we also lead in facing the challenges of deferred maintenance, recruiting and retaining faculty, and competing for the Federal, corporate, and partnership dollars that will help us realize our full vision for workforce development through academic attainment.

Although our Nation's HBCUs make up just 3 percent of colleges and universities, we produce 27 percent of African-American graduates with bachelor's degrees in STEM fields. In addition, the National Science Foundation reports that 21 of the top 50 institutions for educating African-American graduates who go on to receive their doctorates in science and engineering, are HBCUs.

At Grambling State, we are proud to stand as a member of a lean, but mighty force of historically black schools who continue to prove that we are the best partners for addressing America's workforce challenges—most uniquely, those in the fields of cybersecurity and data-driven threat prevention.

As we look forward to a world that is poised to spend $180 billion on cybersecurity in the year 2021, we don't see our challenges, we see an opportunity. With the right and robust support, we know that we are one of America's most critical answers for filling the 3-million-person job gap that exists globally in cybersecurity today.

The investments, that partners like the Department of Homeland Security have the ability to make, will do more than just mitigate the Nation's trillions of dollars in cyber risk. These investments will also substantively change the trajectory of students, families, and the communities who are served by HBCUs. Data from the Social Security Administration shows that your partnership with HBCUs will help raise the average salary of our graduates by more than 40 percent. In addition, studies from McKinsey and Company show us that these more-diverse workforces will help grow company earnings by 14 percent.

When it comes to investing in cybersecurity programs and initiatives at HBCUs, there is only one way to lose—and that is through inaction. We are extremely encouraged by the steps the Members of this committee and leaders throughout our Nation are making to include historically black schools in the conversation about how we best protect our Nation.

The positive vibrations of the work you do here on Capitol Hill will extend all the way to the classrooms and the lives of our students in North Louisiana. When partners like Governor John Bel Edwards and Federal agencies get involved, we are empowered to create opportunities that change the lives of students like Jarrid Richards.

Jarrid is a senior in our computer science program who has ended up in my office with a need many times. He is a great example of how a holistic investment in minority students can help positively impact the trajectory of a person and a company.

During Jarrid's time at Grambling State, there were a few semesters where he encountered a gap, as many of our students do, between Federal aid and his cost to attend. And, while Jarrid worked 3 jobs around campus, there were semesters when without scholarships and grants, he may not have been able to continue his education. When Jarrid was in need of career development, our partnership with CLECO, a local energy provider, was able to provide him his first hands-on experience with network security and preventing cyber threats.

Those investments and the mentorship of his professor Dr. Reddy positioned Jarrid to finish this school year with multiple internships offers and at least two full-time job opportunities that will be waiting when he graduates this fall.

And, while Jarrid's perseverance and grit may stand out among our students, his needs do not. He is much like many students at minority-serving institutions—who just need an opportunity and investment to become the game-changing answers to the needs of American companies and communities today.

It's my extreme honor to lead a university who produces thousands of Jarrids and other innovators who history shows are changing the way our world works. It is my hope that we, Grambling State and other HBCUs, will be offered the opportunity to partner in continuing to secure America's future and producing the workforce talent that will help our Nation remain a leader in innovation.

Thank you.

Mr. RICHMOND. Thank you, Mr. Gallot.

All right. I now recognize Ms. Estwick to summarize her statement in 5 minutes.

STATEMENT OF AMELIA ESTWICK, NATIONAL CYBERSECURITY INSTITUTE, EXCELSIOR COLLEGE

Ms. ESTWICK. Thank you, Chairman Richmond and Ranking Member Katko, and esteemed Members of the subcommittee.

I am proud and honored to appear before you today to discuss the challenges for growing and diversifying the cyber talent pipeline. As the director of the National Cybersecurity Institute at Excelsior College, I will speak passionately on this topic from my perspectives as a black woman, United States Army veteran, cybersecurity practitioner, computer science researcher, educator, and lifelong public servant.

My career began in the early 1990's, when I enlisted in the United States Army, to work in the information security field. During the Gulf War, it became clear that safeguarding and protecting our data and resources was paramount to our National security. Since then, I have earned my bachelor's, master's, and doctorate degrees in computer science, thanks to earning a National Physical Science Consortium fellowship that was sponsored by the National Security Agency while working as a civilian in the intelligence community.

While 30 years have passed since my entry in the field, I still have that same sense of urgency. This is why I feel growing and diversifying the cyber talent pipeline is one of the most important work force issues we address today.

The recent Executive Order on America's cybersecurity work force highlights some important programs that the Federal Government will explore in the near future. As we work collaboratively to address work force needs, I would like to recommend a focus on continued support for initiatives that are already facilitating the growth and diversification of the cyber talent pipeline.

For one, the importance of higher ed. The job market is changing rapidly, and occupations in multiple disciplines increasingly require technological ability, communication skills, and post-secondary degrees. Associate degrees are often great pathways to entry-level employment, and recent statistics state 40 percent of people who earn associate degrees go on to earn higher degrees.

Working adults can leverage their compensation from work and tuition assistance benefits from employers to further their education, and on-line models, like Excelsior College, provide the flexibility required to continue education while working.

Second thing is creating opportunities for current Federal employees to earn academic credentials. According to a recent OPM profile of Federal civilian nonpostal employees, 51 percent of the Federal work force has a bachelor's degree or higher.

In 2014, the OPM created the Federal Academic Alliance to provide higher education opportunities to Federal work force at reduced tuition rates to address the Government-wide skills gap needs, including the shortages in cybersecurity.

Today, OPM endorses 15 colleges and universities, such as Excelsior College, and support for more educational opportunities would be beneficial to the Federal work force.

Three, fostering public and private partnerships. Cooperation of private industry, academia, and Governmental agencies on joint cybersecurity initiatives can take advantage of each sector's complementary strengths. For example, through apprenticeships, internships, and work-study programs, students and employees can get first-hand experience with the cyber threats facing businesses, governments, and nonprofits. Such experiences are particularly important for individuals seeking a career change to access the opportunities in cybersecurity. Also providing employees with opportunities to cross-train will address the upscaling and rescaling needed for creating a pipeline of cybersecurity professionals.

Last, addressing the K–12 cybersecurity education. As an educator and an advocate for equity and inclusion in STEM and cybersecurity, my outreach activities often place me in communities with little awareness about how cybersecurity is applicable to their own lives. This troubles me, because I know that we need to create sustainable STEM and cybersecurity programs that emphasize problem solving, critical thinking, and effective communication skills.

Programs to educate the K–12 ecosystem are important, not only because there is a—a need—excuse me—to protect our digital infrastructure, but also because our youth represent the next generation of cybersecurity professionals.

Mr. Chairman, Ranking Member Katko, and subcommittee Members, in closing, to address the hundreds of thousands of jobs that are currently unfilled and will continue to grow unfilled as technology advances, the work force will need to have the breadth and diversity of initiatives across multiple sectors to support the growth and diversity of the cyber talent pipeline.

This pipeline can be sustained by recruiting, retaining, and advancing populations, such as military and veterans with transferrable skills, individuals from underrepresented groups to include black, Latino, American Indian, Alaskan Natives, funding initiatives to support cybersecurity programs at minority-serving

institutions, and support for advocacy groups whose focus on broadening participation within the cybersecurity field, such as Women in Cybersecurity and International Consortium of Minority Cybersecurity Professionals.

Cybersecurity is a shared responsibility, and until we collaborate at all levels, to include local, State, and Federal, we will continue to operate in silos with the same results in the demographic composition of our work force.

I thank the Chairman and the Ranking Member and the subcommittee for this extraordinary opportunity in providing me with not only a seat at the table, but also a voice.

I am looking forward to answering any questions you may have. Thank you.

[The prepared statement of Ms. Estwick follows:]

PREPARED STATEMENT OF AMELIA ESTWICK

MAY 21, 2019

Thank you, Chairman Richmond, Ranking Member Katko, and Members of the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation. I am proud and honored to appear before you today to discuss the challenges for growing and diversifying the cyber talent pipeline. According to the 2018 (ISC)^2 Cybersecurity Workforce Study, the shortage of cybersecurity professionals is close to 3 million world-wide, with a shortfall of approximately 500,000 in North America. In addition, the report states "63 percent of respondents report that their organizations have a shortage of IT staff dedicated to cybersecurity while 59 percent say their companies are at moderate or extreme risk of cybersecurity attacks due to this shortage." Technology has become ubiquitous and necessary for conducting every facet of our daily lives; however, with the ever-present host of cyber threats our Nation is facing, it is imperative we have a workforce that is skilled and educated to address cyber threats as well as our future technological needs.

My name is Dr. Amelia Estwick, director of the National Cybersecurity Institute (NCI) at Excelsior College and faculty program director for the Excelsior College School of Graduate Studies' Master of Science in Cybersecurity Program. Prior to my academic position, I spent more than 20 years in Government service within the intelligence community (National Security Agency) and Uniformed Services (United States Army). I was the first African-American woman to graduate from NSA's Computer Network Operations Development Program, which was a 3-year intense cyber operations technical leadership program focused on all aspects of cyber operations to include: Attack, exploitation, and defense. At NSA, I held multiple technical leadership positions, including computer science researcher and senior cybersecurity analyst, and prior to my departure in 2016, I was one of the few women technical directors within NSA's Cyber Threat Operations Center; a 24/7/365 cyber operations center responsible for monitoring and defending Department of Defense (DoD) networks globally. For me, reaching the technical director position was a great achievement, considering research by (ISC)^2 show that while "minority representation within the cybersecurity field is slightly higher (26 percent) than the overall U.S. minority workforce (21 percent) . . . racial and ethnic minorities tend to hold non-managerial positions, and pay discrepancies [prevail], especially for minority women." Although I've had a rewarding Government career, my concern for the lack of diversity amongst the cybersecurity workforce ultimately drove me to leave Government service and join academia to help with the Nation's need to grow and diversify the cybersecurity talent pipeline.

In 2013, I joined Excelsior College as an instructional faculty member and subject-matter expert for their graduate cybersecurity courses. In 2016, I decided to join the college full-time as the NCI director and cybersecurity thought leader because I believed in its mission to provide educational opportunities to adult learners through their on-line programs who live across the United States and internationally. This call to service rang especially close to my heart as a veteran and knowing how important it is to provide educational services to active military members who may be stationed in remote locations. In 2014, NCI was established as an academic, training, and research center dedicated to assisting Government, industry, military, and academic sectors meet the challenges in cybersecurity policy, technology, and edu-

cation. In addition, as part of its continuous efforts to build the cybersecurity workforce and influence an informed leadership base that implements cutting-edge cybersecurity policy, NCI launched its Initiative for Women in Cybersecurity (NCI's IWICS). As the director of NCI, I have been instrumental in collaborating with organizations, such as Women in Cybersecurity (WiCyS) and the International Consortium of Minority Cybersecurity Professionals (ICMCP) to promote activities focused on recruiting, retaining, and advancing women and minorities in cybersecurity.

CYBERSECURITY ACROSS THE ACADEMIC CURRICULUM

In March 2018, the Journal of The Colloquium for Information System Security Education (CISSE) published an article "What Constitutes Core in a Cyber Security Curriculum?" which discussed how expansive the cybersecurity field is and stressed the importance of academic institutions taking a multidisciplinary approach to teaching cybersecurity concepts. Cybersecurity curricula was originally rooted in computer science and technology programs; however, the operationalization of cybersecurity in our digital society has necessitated the expansion of a multidisciplinary curricula throughout the academic landscape. This expansion has impacted all disciplines to include business, law, health, and finance.

Cybersecurity's multidisciplinary approach is further supported by the National Information Assurance (IA) Education and Training Programs (NIETP), which manages the National Centers of Academic Excellence (CAE) programs designated by NSA and the Department of Homeland Security (DHS). The goal of the CAE program is "to reduce vulnerability in our National information infrastructure by promoting higher education and research in Cyber Defense (CD) and to produce a growing number of professionals with expertise in CD disciplines". U.S. academic institutions whose cybersecurity programs meet the rigorous criteria to be either a CAE in Cybersecurity Defense Education (CDE), Cyber Operations (CO), or Research (R) are given this designation for a specified amount of years (usually 5 years) and an institution must apply for redesignation before it expires. Institutions with the CAE designation serve as National models for capacity-building of information security programs in higher education, while at the same time strengthening the Nation's infrastructure. CAE-designated institutions benefit from internal and external recognition for faculty and graduates, collaboration opportunities with other CAE-designated institutions, and funding from Federal, State, and local organizations. According to the National Centers of Academic Excellence, more than 230 institutions have been granted the CAE–CDE designation, including Excelsior College which was designated as a CAE–CDE in 2014 (and subsequently redesignated in 2019).

Furthermore, a multidisciplinary approach helps to address the recent Executive Order on America's Cybersecurity Workforce, which proposed an establishment of a cybersecurity rotational assignment program, to serve as a mechanism for knowledge transfer and a development program for cybersecurity practitioners. Providing educational opportunities along with the rotational assignment program will encourage upskilling/reskilling the current Federal and non-Federal workforce to meet the demands of the 21st Century.

THE IMPORTANCE OF PARTNERING WITH COMMUNITY COLLEGES

According to the American Association of Community Colleges' January 2019 report, students enrolled for credit were 56 percent women and 38 percent Hispanic/black. Comparing this to the current demographic statistic from a 2019 (ISC)[2] Cybersecurity Workforce Study on Women on Cybersecurity, women make up 24 percent of the cybersecurity workforce; therefore, partnering with community colleges to create a cybersecurity career pathway could help to diversify the cyber talent pipeline.

There are great benefits to partnerships between community colleges and 4-year colleges that offer on-line education. Associate degrees are often great pathways to entry-level employment. Working adults can then often leverage their compensation from work and tuition assistance benefits from employers to further their education, and on-line models provide the flexibility required to continue education while working. Excelsior College partners with more than 100 community colleges across the United States with 26 of these partners designated as a Center of Academic Excellence for 2-year programs (CAE2Y). Excelsior works with community colleges to evaluate their programs for transfer credit into our Bachelor of Science in Cybersecurity program and help fill the growing need of cyber professionals. In addition, Excelsior provides peer mentoring for community colleges that are working to become a CAE.

FOSTERING PUBLIC/PRIVATE PARTNERSHIPS

In 2014, the Office of Personnel Management created the Federal Academic Alliance (FAA) to provide higher education opportunities to the Federal workforce at reduced tuition rates to address the Government-wide skills gap needs, including the shortages in cybersecurity. Today, OPM endorses 15 colleges and universities, and focuses on providing tuition support to Federal employees, and in many case, their partners and adult children.

With the endorsement of the Chief Human Capital Officers (CHCO) Council, OPM began leading this effort to:

1. Address current Federal-wide and agency-specific skills gaps,
2. Support career development for Federal employees,
3. Provide greater opportunities for Federal employees to obtain college degrees, certificates, and/or college credits,
4. Provide this opportunity with colleges and universities that offer an on-line component to address our world-wide workforce,
5. Provide current college students with a greater understanding of the Federal Government.

Colleges and universities that make up the FAA, such as Excelsior College, are vetted by OPM to ensure they meet mission-critical occupational needs; are in good standing; are not-for-profit; and are regionally accredited. Most FAA member institutions offer cybersecurity and/or information technology certificates and degrees (undergraduate and graduate) to help fill Federal skill gaps. Providing the additional option for certifications helps to support talent development and career advancement opportunities.

EDUCATING STUDENTS TO PREPARE AND PROTECT OUR NATIONAL CRITICAL INFRASTRUCTURES

The number of cyber attacks targeting our Nation's critical infrastructures are on the rise. Specifically, in 2013, 59 percent of the attacks against our critical infrastructure were reported in the energy sector (ICS–CERT, 2013). A skilled and educated workforce is an essential component in improving the security posture of our critical infrastructure. The security program of the nuclear sector is regulated by the Federal Government with governance under the U.S. Nuclear Regulatory Commission (NRC). In addition to being competent in cybersecurity, professionals working in the nuclear and energy industries need to be aware of specific standards, requirements, and unique cyber threats.

Excelsior College has a long history of meeting the educational needs of the nuclear workforce through innovative educational solutions. In 2014, a degree program was created to address cybersecurity challenges facing the nuclear industry. Cybersecurity professionals in the nuclear sector require a broad range of technical skills; however, few college programs currently exist at the baccalaureate level to assure that these professionals have the unique skill sets and knowledge domains needed to protect facilities and our National security. Additionally, the critical and practical nature of nuclear and energy sectors calls for enhanced simulation-based learning to be developed. Due to Excelsior's innovative program, in June 2018, Excelsior College received a Department of Energy Nuclear Energy University Programs (DOE–NEUP) grant to purchase a web-based pressurized water reactor simulator for use in the nuclear engineering technology program. The ~$250K grant provides funding to:

- support plant simulation to enhance student achievement of higher cognitive learning outcomes through "learning by doing,"
- provide the ability to evaluate and analyze technical information during "dynamic" situations
- enhance our student's experiential learning activities, and by doing so, enhance the student's ability to meet industry needs
- enable students to advance their understanding of key theories and concepts in the nuclear technology field to better protect against cyber threats.

The value of Government funding to support the development of these lab-based activities means without such support, higher education institutions might not be able to adopt this important technology. Therefore, there is an increasing need to expand Government funding of experiential learning, especially in an on-line environment, where skills shortages in cybersecurity can only be filled by shifting people from one industry/occupation to cybersecurity fields.

Excelsior works closely with RCNET (Regional Center for Nuclear Education and Training) to partner community colleges and corporations to further advance the integration of cybersecurity measures within the energy field with the support of the National Science Foundation's Advanced Technological Education (ATE) program.

These programs implemented at the College directly address the President's Executive Order (EO) 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure as well as EO on America's Cybersecurity Workforce to identify and evaluate skills gaps for Federal and non-Federal cybersecurity personnel with an emphasis on protecting our Nation's critical infrastructures.

ADDRESSING K–12 CYBERSECURITY EDUCATION

According to Education Superhighway's 2018 State of the States report, "40.7 million more students have high-speed broadband in their classrooms." With more than 44 million students connected to the internet since 2013, this means "98 percent of school districts can take advantage of digital learning." This is an impressive number for schools that can provide digital learning for their students in addition to integrating technology into the classroom as schools become increasingly reliant on technology and sophisticated IT systems for teaching, learning, and school operations. If you consider millions of mobile PCs (such as notebooks/Macs, netbooks, tablets, and Chromebooks) are being purchased by U.S. K–12 schools every year, think about the challenges these schools face trying to secure this infrastructure against cyber threats; a daunting prospect for any school district to counter. Programs to educate the K–12 ecosystem are important not only because there's a need to protect these resources, but also this demographic represents the next generation of cybersecurity professionals.

One program addressing the K–12 population is the NSA/National Science Foundation (NSF) GenCyber Program. The GenCyber program provides summer cybersecurity camp experiences for students and teachers at the K–12 level. "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. GenCyber is providing a solution to the Nation's shortfall of skilled cybersecurity professionals by ensuring that enough young people are inspired to direct their talents in this area, which is critical to the future of our country's National and economic security as we become even more reliant on cyber-based technology in every aspect of our daily lives."

In 2018, Excelsior College partnered with two Boards of Cooperative Education Services (BOCES) serving 46 districts with a combined population of more than 80,000 students throughout New York State's Capital Region to offer one teacher camp for middle and high school educators. The GenCyber ~$100K grant provided Excelsior College and BOCES an opportunity to offer the first GenCyber cybersecurity camp in the New York State Capital Region. The camp taught 30 middle and high school educators from different disciplines and diverse populations about foundational cybersecurity concepts. GenCyber programs support the President's EO on America's Cybersecurity Workforce on developing and implementing educational programs for K–12 which is proposing to reward an annual Presidential Cybersecurity Education Award to elementary and secondary school educators who best instill skills, knowledge, and passion with respect to cybersecurity and cybersecurity-related subjects.

EXPANDING OPPORTUNITIES FOR EXPERIENTIAL LEARNING

One of the keys to cybersecurity education is ensuring students are prepared upon graduation with practical, hands-on skills. Employers need employees with competencies that are directly related to the threats they encounter within their organizations. Opportunities for experiential learning allows the student to not only gain real-world experiences but also the ability to reflect on those experiences and build on their knowledge is important for reskilling/upskilling cybersecurity professionals. Some examples of experiential learning are:

Cyber Competitions / Capture-the-Flag (CTFs) / Cyber Ranges

Cyber competitions originated from cyber defense exercises that were traditionally designed by the U.S. military service. Over the years, cyber competitions or CTFs have become increasingly popular for students to partake in to assess their competencies and skills. The challenges are designed to replicate the type of threats that are prevalent in the workplace and participants compete with other college teams to identify and capture flags within the exercises. Besides the hands-on experiences, students benefit from each other in acquiring the soft skills that are sometimes lacking in the technical arena, such as: Teamwork, leadership, communication, and problem solving which are all crucial skills to have in cybersecurity. The President's EO on America's Cybersecurity Workforce supports a plan to develop "an

annual cybersecurity competition (President's Cup Cybersecurity Competition) for Federal civilian and military employees. The goal of the competition shall be to identify, challenge, and reward the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines." NCI, through our student chapter of the National Cybersecurity Student Association (NCSA), has sponsored Excelsior students for the past 4 years to compete in cyber competitions; which resulted in several of our teams placing among the top 100 National teams.

Apprenticeships/Internships/Work-Study

While colleges and universities can and do infuse lab simulations, tabletop exercises, and case studies within their courses, internships (both virtual and in-person) provide opportunities for students to work within the contexts of the real world. As part of these programs, they can get first-hand experience with the issues facing business, Government, and nonprofits. This is particularly important for individuals looking to change their career to take advantage of opportunities in cybersecurity. At Excelsior College, we have worked on developing an option for students to complete an internship for credit. By participating in internships, students gain practical work experience that they can use to demonstrate their skills and potential to future employers. For employers hosting interns, there is a potential to increase capacity in the short term and build talent pipelines in the long run. The internship course at Excelsior College is a 15-week instructor-led course that runs simultaneous to the internship experience. Students are expected to spend 9 hours per week on their internship experience and work activities and write a weekly reflective journal about the applicability of the experience to their degree program and future career plans.

CONCLUSION

Mr. Chairman, in closing, there are several efforts that support growing and diversifying the cyber talent pipeline; however, we must be mindful of how those programs are executed to ensure equitable representation of women and minorities in the cybersecurity profession. As stated by Rick Ledgett, former deputy director of the National Security Agency, "Getting more women and minorities into that cyber security workforce will be the key to addressing the current and expected labor shortfalls."

With a shortfall of approximately 500,000 North America-based cybersecurity jobs, as a society we should be using all resources at our disposal to provide career pathways to ensure these jobs are filled. For me, it starts with early education at the K–12 level where education can help protect key resources and we are able to build competencies in the next generation of cybersecurity professionals. It continues with partnerships across multiple sectors, where organizations can work together to expand the workforce. And it works best when we have identified the key competencies and skills required to protect our critical infrastructures specifically and our National security generally.

Thank you for the opportunity to testify before you and the subcommittee, and I look forward to any questions you may have.

Mr. RICHMOND. Thank you for your testimony. Thank you for your service. Let me apologize for calling you Ms. Estwick as opposed to Dr. Estwick. It was well-earned, and I should make sure that I call you by that title.

We are going to stand in recess until we go vote. We will be back, hopefully, at somewhere around 15 minutes—on the worst side, maybe about 20, but it is Government, so who knows.

We will stand adjourned—in recess. I am sorry.

[Recess.]

Mr. RICHMOND. We are going to call the subcommittee back to order, and we left off with Ms. Worley.

If you will take the time to summarize your testimony in 5 minutes, we appreciate it.

STATEMENT OF CANDACE WORLEY, VICE PRESIDENT AND CHIEF TECHNICAL STRATEGIST, MC AFEE

Ms. WORLEY. Mr. Chairman, Ranking Member Katko, and Members of the subcommittee: Thank you for the opportunity to testify today. I am Candace Worley, vice president and chief technical strategist for McAfee, a device-to-cloud cybersecurity company.

I am pleased to address the subcommittee on the need to grow and diversify the cybersecurity talent pipeline. It goes without saying that every cybersecurity organization, including Government, suffers from a shortage of cyber talent.

No matter how committed we are to the cause of securing the digital world, we have to have enough people, we need to train enough people to fill these jobs.

It is not just about filling security roles. There is an economic element to the cybersecurity challenge. McAfee worked with CSIS in 2018 to refresh a study that we initially did in 2014 around the economics of cyber crime. That research showed that cyber crime is worth approximately $170 billion in GDP annually in North America and between $400- and $600 billion globally.

If we can recapture even half of that money back into the positive side of our economy, that would be a huge growth engine for North American economy as well as the global economy. We will not be able to do that unless we have cyber professionals available and in organizations to help secure both Government and the private sector against those attacks.

Today, I will make 5 recommendations for addressing the cybersecurity talent shortage challenge.

First, we must increase the CyberCorps Scholarship for Service program, SFS, which is administrated through the National Science Foundation, and provides grants to approximately 70 institutions across the country, enabling 10 to 12 students per institution to get those scholarships. After they graduate, these students go to work in the Government for at least the same amount of time as they receive support in their education.

What we found is that they tend to remain in the Federal Government even longer. So this program is not only a great program for the student, it also enables the Federal Government to compete more readily with private industry for those employees. Because they are already employees of the Federal Government, they tend to stay longer.

Since fiscal year 2018, the program's funding has remained flat at $55 million annually supporting these scholarships. That allows about 2,000 students to get scholarships. We are recommending that Congress should increase these, funds to around $200 million annually, which would enable about 6,400 students to receive scholarships and continue to enable the Federal Government with cybersecurity talent.

SFS should also be made available to more than just the current 70 land grant institutions. This stipulation is needlessly limiting, if we really want to increase the talent pool.

Second, we must expand the SF program to community colleges, where approximately 57 percent of students are women and 41 percent are minorities. Additionally, many individuals, who are going back to retrain for a second or third career, choose a community

college rather than a 4-year institution. That population has great experience that could be relevant in addition to the cybersecurity curriculum for filling open roles.

Third, a strong cybersecurity operation requires different levels of skills. Not everyone needs a Ph.D. or a computer science degree to work in a security operations center. We, in industry, and Government, should be considering our hiring requirements, and opening those requirements up to people beyond those that just have a degree, for certificate and other training programs, can do the job just as well for many of the positions that are open. In fact, we may also contemplate other opportunity for vocational programs to be developed.

Fourth, to ensure we are coming up with the most creative solutions possible to address current and future cybersecurity challenges, we must focus on a diverse pipeline of talent. We need people with diverse perspectives and capabilities who can think critically about the cybersecurity problems. That talented pool should be diversified from many perspectives. Certainly race, gender, experience, but also looking at people like gamers, veterans, retirees, who bring a unique set of experiences and capabilities to the discussion.

Finally, we must develop creative approaches to enabling a public and private partnership, particularly during significant cybersecurity events where we need that collaboration in order to solve serious problems.

We should design a mechanism for cyber professionals to move back and forth between the public and private sector so that Government organizations would have a continual refresh of expertise.

The Executive Order on America's cybersecurity work force, issued earlier this month, is a good step in that direction. We also support wide-spread adoption of the Cybersecurity Workforce Framework developed by the National Initiatives for Cybersecurity Education.

At McAfee, we are walking the walk when it comes to implementing solutions to increase diversity and inclusion among our ranks. We achieved pay parity, making McAfee the first pureplay cybersecurity company to do so. To recruit diverse talent, we ensure job descriptions have inclusive language, and recruiters understand diversity and value-based interviewing as an integral part of our process.

We also invest in enabling our employees to take time to train local high schools and grade schools on an on-line safety program that we have developed targeting children so that they better understand the risks associated with the digital world.

Feeding the pipeline with smart, talented, and diverse individuals is critical to developing and maintaining the next generation work force that will defend American companies and the Government from growing cyber threats.

Thank you for your interest in this topic, and I will be happy to answer questions as it proceeds.

[The prepared statement of Ms. Worley follows:]

PREPARED STATEMENT OF CANDACE WORLEY

MAY 21, 2019

Good afternoon, Chairman Richmond, Ranking Member Katko, and Members of the subcommittee. Thank you for the opportunity to testify today. I am Candace Worley, vice president and chief technical strategist of McAfee, LLC.

I am pleased to address the subcommittee on the need to grow and diversify the cyber talent pipeline. My testimony will address the cybersecurity skills gap and workforce shortage, the need for investment in training programs and cross-training more cyber experts, the role the Federal Government can play to grow a diverse cyber workforce generation and how we can work together to address the challenges we currently face to diversify and grow the talent pipeline.

First, I would like to provide some background on my experience and McAfee's commitment to cybersecurity and developing a diverse cyber workforce. At McAfee, I manage a world-wide team of technical strategists who drive thought leadership and advance technical innovation in McAfee security solutions. I have held a number of technology leadership positions, including 5½ years as the vice president and general manager of McAfee's Enterprise Endpoint Security business.

MC AFEE'S COMMITMENT TO CYBERSECURITY AND GROWING THE TALENT PIPELINE

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates enterprise and consumer solutions that make our world a safer place for the benefit of all. Our holistic, automated, open security platform and cloud-first approach to building security solutions allow all security products to coexist, communicate, and share threat intelligence with each other anywhere in the digital landscape. Our customers range from Government agencies to all sizes of business to millions of home users.

We and every other cybersecurity organization, including the Government, suffer from a shortage of talent. No matter how committed we are to the cause, if we want to truly make the world safer, we must train more people to fill the jobs that ensure our security.

THE CYBERSECURITY TALENT GAP

In 2016 the Center for Strategic and International Studies (CSIS) and McAfee undertook a study titled *Hacking the Skills Shortage* based on a global survey of IT professionals. Some of the findings about the cybersecurity talent gap include:

- 82 percent of those surveyed reported a lack of cybersecurity skills within their organization.
- 71 percent agreed that the talent shortfall makes organizations more vulnerable to attackers, and 25 percent say that lack of sufficient cybersecurity staff has actually contributed to data loss or theft and reputational damage.
- 76 percent of respondents said their governments are not investing enough in programs to help cultivate cybersecurity talent and believe the laws and regulations for cybersecurity in their country are inadequate.

Since that study nearly 3 years ago, the numbers haven't improved. According to a recent (ISC) study, the global cybersecurity workforce shortage has reached 2.93 million professionals. The cybersecurity skills shortage is equally troublesome within the Federal Government.

Given the vital role Government agencies such as the Departments of Defense, Homeland Security, as well as the intelligence agencies play in protecting the United States, policy makers must address the skills gap and work to reduce it.

Recent Administration Efforts

The President's Executive Order on America's cybersecurity workforce, issued earlier this month, is a critical step toward helping solve the cybersecurity skills shortage. As a cybersecurity company, McAfee is a strong proponent of the wide-spread adoption of the cybersecurity workforce framework created by the Department of Homeland Security's (DHS) National Initiative for Cybersecurity Education (NICE) and supports the development of a rotational program for Federal employees to expand their cybersecurity expertise. McAfee has aligned the skills it seeks in candidates and its job requirements with the NICE guidelines.

We are also encouraged by the creation of the President's Cup Cybersecurity Competition designed to reward top cyber performers. This program was modeled after successful private-sector initiatives and shows how cross-sector collaboration is essential to alleviating the cybersecurity workforce shortage. It is critical that we work to eliminate barriers for those entering the cybersecurity fields and increase

educational opportunities to ensure talented people from diverse backgrounds can fill the growing IT and cybersecurity talent deficit.

The administration's Executive Order is a step forward; however, it can't on its own solve the issue of a dwindling cybersecurity workforce. We have long advocated for eliminating barriers to entering the cybersecurity fields, and we encourage the Government to support programs that increase educational opportunities to ensure talented people from diverse backgrounds can join the growing cyber industry.

Following are some recommendations for training and incentivizing more people to enter the cybersecurity field.

RECOMMENDATIONS

Increase the NSF CyberCorps Scholarships for Service Program

To grow the talent pipeline and close the cyber workforce gap, Congress should focus on expanding existing programs that train students in the fields valued by the cybersecurity industry.

The CyberCorps Scholarship for Service (SFS) program is designed to increase and strengthen the cadre of Federal information assurance specialists that protect Government systems and networks. The program, administered through the National Science Foundation (NSF), provides grants to about 70 institutions across the country to offer scholarships to 10–12 full-time junior and senior college students each. With this structure, students are awarded free tuition for up to 2 years in addition to annul stipends—$22,500 for undergraduates and $34,000 for graduate students. There are also allowances for health insurance, textbooks, and professional development.

Upon completing their coursework in areas relevant to cybersecurity and a required internship, students earn their degrees and go on to work as security experts in a Government agency for at least the amount of time they have been supported by the program. After that, they can apply for jobs in the public or private sector.

To date, the Federal Government has made a solid commitment to supporting the SFS program. The program was funded at $55 million in 2019 and NSF is requesting the same amount for their 2020 budget. At a baseline, an investment of $50 million pays for roughly 2,000+ students to complete the scholarship program. We can do better!

Given the substantial cyber skills deficit, policy makers should significantly increase the size of the program to the range of $200 million. If this level of funding were appropriated, the program could support roughly 6,400 scholarships. This investment would make a dent in the Federal cyber skills deficit, estimated to be in the range of 10,000 per year by Tony Scott, then Federal CIO, in 2015. Unfortunately, the 10,000-person talent deficit continues to exist today.

At the same time, this level of investment could help create a new generation of Federal cyber professionals who could serve as positive role models for middle and high school students across the country to consider the benefits of a cyber career and Federal service. On a long-term scale, this positive feedback loop of the SFS program might be its biggest contribution.

While the CyberCorps SFS program is laudable, it is currently available only to 70 institutions—and all are land grant colleges. Current law limits SFS scholarships to research universities. This policy needlessly limits access to scholarships for qualified students from hundreds of universities and colleges around the country. In addition to expanding the funding, the scholarship program should be expanded to include other learning institutions, given the large number of talented and deserving students in our country.

Expand the NSF CyberCorps Scholarships for Service Program to Community Colleges

We should consider expanding—or creating a similar program—for community colleges. If we are going to close the cybersecurity talent gap across the country, we should focus resources on students pursuing associate degrees, which are valued in an industry that does not necessarily require a PhD or 4-year computer science degree. A strong security operation requires different levels of skills, and having a flexible scholarship program at a community college could benefit a wide variety of applicants while providing the profession with other types of necessary skills.

Community colleges also attract different types of students than 4-year institutions. Some are recent high school graduates, but many are working adults and returning students looking for a career change or valuable skills training.

Recruiting from community colleges would further a diverse cyber workforce. Data shows that 57 percent of community college students are women and 41 percent are minorities. Additionally, community college tuition is more economical than a 4-year

university. In-State community college tuition is about one-third the cost of in-State 4-year colleges, meaning the scholarship funds would go further with a program focused here.

Such an expanded program, through a public-private partnership, could attract high school graduates who don't yet have specific career aspirations into focusing on cybersecurity. The Federal Government could fund all or part of the tuition remission for students, while private companies could help develop coursework in cybersecurity. Interested students would have the opportunity to learn from college faculty and private-sector practitioners.

For example, an IT company could offer several faculty members or guest lecturers to participate during a semester. Students would receive free tuition—paid by a Federal program, perhaps with private-sector contributions—but would not receive a stipend for living arrangements, as 4-year college students do in the CyberCorps program. Students would receive a 2-year certificate in cybersecurity that would be transferrable to a 4-year school. Like the CyberCorps program, graduates would spend the same amount of time as their scholarship period working in a guaranteed Government job.

A program like this has the benefit of bringing in private-sector experts, interesting younger students who have not yet made a career commitment, interesting veterans, attracting a diverse range of students, and likely costing the Government less—once the start-up costs are accounted for. Such a program should not substitute but rather complement the existing, highly-valued CyberCorps SFS program.

Furthermore, a candidate should not need to have a degree or certificate from a college to be a well-trained cybersecurity professional. Certificate programs provide valuable training, and there are increasingly more of these. In order to take advantage of these individuals, however, governments and businesses would have to change their hiring requirements. It is not necessary to have a college degree to work in cybersecurity, and requirements should be updated to reflect that.

Foster Diversity of Thinking, Recruiting, and Hiring

Cybersecurity is one of the greatest technical challenges of our time, and we need to be as creative as possible to meet it. In addition to continually advancing technology, we need to identify people from diverse backgrounds—and not just in the standard sense of the term. We absolutely need to diversify the talent pool in terms of race, ethnicity, gender, and age, all of which lead to creating an inclusive team that will deliver better results. Research on large, innovative organizations has shown that gender and racial diversity improves organizations' financial performance. The title of this article in Scientific American States the case well: How Diversity Makes Us Smarter: Being around people who are different from us makes us more creative, more diligent and harder working. McAfee believes we need to focus on hiring a diverse workforce, which will in turn make us an even stronger company.

There are, however, additional ways to diversify our talent pool. We should seek out gamers, veterans, people working on technical certificates, retirees from computing and other fields such as psychology, liberal arts as well as engineering. There is no one background required to be a cybersecurity professional. Of course we need people with deep technical skills, but we also need teams with diverse perspectives and capabilities.

Cyber attacks are diverse and complex, ranging in scope from organized crime to recreational vandalism to hacktivism to State-sponsored initiatives. Orchestrating a robust cyber defense requires a breadth and depth of backgrounds, skills, and experiences to respond to and mitigate innumerable threats, many of which haven't even been invented yet.

When looking for cybersecurity talent, it's easy to ask, "What degrees are needed?" or "What certifications should be required?" But cyber moves quickly; we need people who can think and move quickly with it. McAfee's CTO Steve Grobman once said, "Computer Science is a great field for people who hate to be bored." Degrees and certifications are a great way to demonstrate current knowledge. Yet when I'm hiring, I care less about what you know now than what you have the capacity to understand and respond to 2, 3, or 5 years from now. Technology will change, the infrastructure will change, but the need to think critically and respond to a variety of challenges will not change. Complexity will only increase, and we need cybersecurity professionals who will evolve with it.

Public-Private Sector Cross-Pollination

We also must develop creative approaches to enabling the public and private sectors to share talent, particularly during significant cybersecurity events. We know that the adversary is constantly innovating and changing course, often reacting to

new defensive capabilities the private sector develops. It's unrealistic to think that Government cyber practitioners would be able to keep up with such a rapidly evolving environment without private-sector assistance. We should design a mechanism for cyber professionals—particularly analysts or those who are training to become analysts—to move back and forth between the public and private sector so that Government organizations would have a continual refresh of expertise.

One way to accomplish this would be for DHS to partner with companies and other organizations such as universities to staff a cadre of cybersecurity professionals—operators, analysts, and researchers—who are credentialed to move freely between public and private-sector service. These professionals, particularly those in the private sector, could be on call to help an impacted entity and the Government respond to a major attack in a timely way.

Both Government and private-sector cybersecurity professionals would benefit from regular job rotations of possibly 2 to 3 weeks each year. This type of cross-pollination would help everyone share best practices on technology, business processes, and people management. DHS should include a flexible, public-private pool of certified professionals in its plan to rewrite its cybersecurity hiring and retention plan. If DHS is not ready to act, Congress should establish a blue-ribbon panel of public and private-sector experts to study how a flexible cadre of cybersecurity professionals could be started and managed. Much like the National Guard, a flexible staffing approach to closing the skills could become a model of excellence.

HOW TECHNOLOGY CAN HELP ALLEVIATE THE PROBLEM

Even though we should work hard and think creatively to fill it, the cyber skills gap won't be closed any time soon. In the mean time, we must rely on technology more and more.

Human-Machine Teaming

One strategy for addressing the cybersecurity skills deficit is to use automation—through such solutions as machine learning and artificial intelligence. Legacy IT systems, however—like many of those in the Federal Government—lack the ability to take advantage of the most contemporary security architectures and development techniques. While it is possible to isolate or wrap security around a legacy system, the approach is far inferior to a well-designed secure implementation designed for the security challenges of 2019 and beyond.

This speaks to the need for investments in IT modernization and modern cybersecurity solutions, which an earlier Executive Order addressed. We support these much-needed policy changes, which will allow for better use of automation, or machine learning.

The ideal situation for now is what McAfee calls human-machine teaming. This means taking advantage of the particular strengths of each. Machine learning can save security teams both time and energy, as it is the fastest way to identify new attacks and push that information to endpoint security platforms. Machines are excellent at repetitive tasks, such as making calculations across broad swaths of data. That's one of the strengths of machine learning: Its ability to crunch big data sets and draw statistical inferences based on that data, detecting patterns hidden in the data at rapid speed.

Humans, on the other hand, are best at insight and analysis. With the assistance of machine learning, human analysts can devise new defenses quickly, adapting to attackers' automated processes and limiting their effectiveness. The human intellect is capable of thinking like an adversary and understanding a scenario that might never have been executed in any environment previously. Machines can take over some simple processes—automating them so the humans can be free to understand context and implication, such as why a bad actor might want to attack a Government agency.

MCAFEE'S COMMITMENT TO CLOSING THE SKILLS GAP

While we recognize there is still more to do, we're proud to describe the strides we're making at McAfee. We believe we have a responsibility to our employees, customers, and communities to ensure our workplace reflects the world in which we live. Having a diverse, inclusive workforce is the right thing to do, and after we became an independent, stand-alone cybersecurity company in 2017, we made and have kept this a priority.

At McAfee, we're walking the walk when it comes to implementing solutions to increase diversity and inclusion among our ranks. This business model is essential to the cybersecurity industry's success. Studies show time and again that diverse

perspectives and human experiences lead to more creative approaches to solving challenges, and we know that inclusive teams deliver better results.

Pay Parity

Our most recent accomplishment was to audit our global employee base to look into pay parity. In April 2019 we achieved pay parity, making McAfee the first pureplay cybersecurity company to do so. It required an investment of $4 million to make salary adjustments on April 1. We'll continue to adjust the pay gap and uphold pay parity with annual analysis.

Holding Ourselves Accountable

In 2018, our first year as an independent company, we released our first Inclusion and Diversity Report. The report demonstrates our commitment to building a better workplace and community. Highlights include:

- In 2018, 27.1 percent of all global hires were female and 13 percent of all U.S. hires were underrepresented minorities.
- In June 2018, we launched our "Return to Workplace" program for men and women who have paused their career to raise children, care for loved ones, or serve their country. The 12-week program offers the opportunity to reenter the tech space with the support and resources needed to successfully relaunch careers. As a result, 80 percent of program participants were offered a full-time position at McAfee.
- Last year, we established the Diversity & Culture Council, a volunteer-led global initiative focused on creating an infrastructure for the development and maintenance of an integrated strategy for diversity and workplace culture. Council responsibilities include implementing a company-wide inclusive culture by supporting diversity goals, providing a platform for open and efficient employee feedback, and enabling best-practice sharing from local sites on company initiatives.
- McAfee CEO Chris Young joined CEO Action for Diversity Inclusion, the largest group of CEOs and presidents committed to act on driving an inclusive workforce. By taking part in CEO Action, Young personally commits to advancing diversity and inclusion with the coalition's three-pronged approach of fostering safe workplaces:
  - Create and maintain trusting workplace environments that support open dialog,
  - Share best practices and lessons from unsuccessful practices for others to learn from,
  - Implement and expand unconscious bias education.

When hiring new talent, we keep to these principles:

- *Inclusive language in job descriptions*.—We leverage tools to better understand the impact of our language in job descriptions. After analysis, we made alterations that now offer gender-neutral language that speaks to all candidates.
- *Recruiters who know diversity*.—Our dedicated team of trained recruiters know where to show up and more importantly, how to show up, to recruiting events. In 2018, we expanded our team focused on diverse hiring to bring top talent into our pipeline.
- *Values-based behavioral interviewing*.—All recruiters and hiring managers are trained to use our values-based behavioral interview approach, which encourages interviewers to ask questions related to our values, resulting in more meaningful interactions.
- *Diverse representation on hiring panels*.—We have trained more than 60 female employees in values-based behavioral interviewing, and we leverage them across the globe to ensure diverse representation on each interview panel.
- *Referral bonuses for diverse hires*.—In 2018, we launched a global referral bonuses for hires of female employees into the Sales organization. As a result, our Sales organization experienced a 131 percent increase in new female hires.
- *Outreach at conferences and events*.—In 2019, we plan to continue our investment in events that focus on diversity and will hone our approach, so we attend fewer, more strategic events and build stronger relationships.

Investing in the Next Generation Workforce

Investing in a diverse pipeline is essential to the development of a strong cyber workforce for the future. McAfee is proud to support the community to establish programs that provide skills to help build the STEM pipeline, fill related job openings, and close gender and diversity gaps. These programs include an On-line Safety Program, on-site training programs, and internships for high school students. Our employees also volunteer in schools help educate students on both cybersecurity risks

and opportunities. Through volunteer-run programs across the globe, McAfee has educated more than 500,000 children to date.

As part of the McAfee's new pilot Achievement & Excellence in STEM Scholarship program, McAfee will make 3 awards of $10,000 for the 2019–2020 school year. Twelve students from each of the 3 partner schools will be invited to apply, in coordination with each partner institution's respective college advisor. Target students are college-bound, high school seniors with demonstrated passion for STEM fields, who are seeking a future in a STEM-related path. This type of a program can easily be replicated by other companies and used to support the growth and expansion of the workforce.

NEXT STEPS TO ADDRESS THE CHALLENGES

Finally, I would like to stress the importance of allocating time for advocacy by current cyber professionals to recruit and retain the next generation. As a woman in tech, I know first-hand the pressure to prove yourself—not only for your own career success, but as a representative of your culture or gender. It can be extremely difficult to deliver excellence in your day job and carve out time to engage and lift up the next generation. If we are going to inspire and empower a new and diverse corps of cybersecurity professionals, we must prioritize time for current role models to advocate, inspire, and recruit.

McAfee strongly recommends that any future initiative include commitments by industry to provide diverse technical professionals—not only by gender and race, but skillset and experience—to teach and mentor. We also recommend that students accepted into a CyberCorps program spend time teaching cyber safety to America's K–12 youth. When we build an entire continuum—each stage of cybersecurity experts uplifting and empowering the generation after it—then we will truly, systemically achieve our National objective.

CONCLUSION

It has been an honor to appear before this distinguished panel of policy makers. Thank you, Chairman Richmond and Ranking Member Katko, for your dedication to growing and diversifying the cybersecurity workforce. Feeding the pipeline with smart, talented, and diverse individuals is critical to developing and maintaining the next generation workforce that will defend American companies and the Government from growing cyber threats. The future of cybersecurity can be bright, if we're able to harness the potential of all people to create a growing and diverse talent pipeline.

In the near future, I hope that we think of cyber as one of the most diverse fields of people and skill sets who will meet the challenges of protecting public and private-sector institutions from an array of cybersecurity threats. We should increase the NSF CyberCorps Scholarships for Service Program to include more students, encourage students from community colleges to pursue careers in cyber, and focus on diversity and inclusion in the pipeline.

Thank you, and I'll be happy to answer any of your questions.

Mr. RICHMOND. I want to thank all of the witnesses for their testimony. I will remind each Member that he or she will have 5 minutes to question the panel.

I will recognize myself. I will yield it to Ms. Slotkin. Other than that, we may not have the time to get you in and out of here. So I will yield my time to Ms. Slotkin.

Ms. SLOTKIN. Thank you, Mr. Chairman.

So I am from Michigan, and in my district, we have this fantastic cybersecurity program at one of our local high schools. I went and visited there. So young people are literally starting to learn to code and to do all of the sort-of training for cybersecurity experts. They are being recruited straight out of college, right? Some of them are being asked to forego any higher education just because we are so desperate in Michigan for cybersecurity talent.

So tell me what more we can be doing, particularly in rural areas, right. The high school I am talking about is a rural school, and it has been a fantastic program for us.

Tell me what I can do if I have rural schools who want their kids to go into this desperately-needed job, but they just don't know where to look first?

Mr. GALLOT. Well, I guess I will just jump in real quick.

I think creating partnerships and pipelines within education is a key. One of the things that we do in—in Louisiana, we have got Bossier Parish Community College that provides an associate's degree. Grambling will have the bachelor's degree; Louisiana Tech, 5 miles down the road, has a master's program.

So creating the pipeline from that high school to either a community or junior college and then to university, I think, is something that has worked for us. When you think about the support we provide at Cyber Innovation Center, Barksdale Air Force Base in Bossier City, and the other private companies in that area, I think creates a good pipeline and a diverse pipeline of cybersecurity workers.

Ms. SLOTKIN. I apologize. We mentioned this when I wasn't here. But, you know, we have experience, particularly in the U.S. military, with saying certain career fields are really in desperate need, and we have incentives for people to join the military, they have special skills, like if they speak Chinese or Russian.

Can you tell me what you would do to incentivize, particularly the military and Government agencies, since we often lose out to private sector who pay better?

Mr. SIMPSON. Sure. I will jump in here on this one. So there are a lot of great transitioning veteran programs out there. So there are a number of States that we currently work with at (ISC)^2, that we work with that are funded by the actual State for transitioning veterans.

So there is programs already set up, they are already in place. They are very, very successful——

Ms. SLOTKIN. Sorry. Just because I have a short time, not to help the veterans when they get out, because I have certainly seen a lot, but to get them in—like to get them in the uniformed military, to get them in the Federal agencies, since cybersecurity is going to be the battlefield of the future, and we don't pay as much—I am a former Federal Government employee. We don't pay as much as the private sector for a cybersecurity professional. What should we be doing in the Federal Government to incentivize getting people in rather than when they are done? Helping them out?

Ms. WORLEY. Certainly on the topic of getting them in the Federal Government versus the services themselves, I think the SFS program is a great way to do that. Continuing to fund that program to a greater degree, where I give you 2 years of college, you give me 2 years of service in the Federal Government, right? Now you have them working in the Federal Government, they understand that mission, they get a feel for what it is like to work in Government. We saw some stats at about 70 percent of those who go into the Federal Government in that program stay for at least a year longer.

So I think the program that you currently have in place is actually serving that goal pretty well. On the front of military, I think that may be a more difficult challenge. But certainly, I think, this program is helping you at the Federal level.

Ms. SLOTKIN. Thank you.

Mr. Chairman, I yield back.

Mr. RICHMOND. Ms. Estwick, did you——

Ms. ESTWICK. No, that is OK. No. So I just wanted to add one thing about earlier when you talked about the K–12. So I don't know if you are familiar with the NSA, National Security Agency, National Science Foundation's GenCyber program. That is a program that has been around for about, I want to say, 5 to 6 years now.

They do K–12 camps, student camps, and teacher camps, and they award various organizations—you can be a nonprofit and schools—Excelsior College, we were actually awarded a grant last year, and we held a cybersecurity camp for middle and high school teachers in the New York State capital region. What that does, they have goals in mind, of course, to increase interest in cybersecurity, but other goals, of course, is to diversify the work force.

There is just—just a host of opportunities there for kids. Exposure is the thing, right? So you want to make sure you get as much exposure. Of course, there is cyber competitions as well, cyber patriot programs and things like that as well.

Ms. SLOTKIN. Thank you.

Mr. RICHMOND. The gentlelady yields back.

I now recognize the gentleman from New York, Mr. Katko.

Mr. KATKO. Thank you, Mr. Chairman.

I want to start with Ms. Worley, but actually this question applies to everybody.

I think the National Science Foundation CyberCorps scholarships are a great place to start, because they have a time commitment after they get the scholarship.

Are any of you aware of any problems with implementing, or getting enough professors involved, or enough universities involved? Is anybody aware of any problems with that part of it?

Ms. WORLEY. So what I would say is that I see an increased number of educational institutions, certainly at both the—the university as well as the community college level, who are beginning to implement cybersecurity programs, either as an augmentation to existing computer science and engineering programs, or as a pure cybersecurity program. So I am certainly seeing increased interest in availability, but I am sure other folks——

Mr. KATKO. I guess my question is really focused that—there is requirements that go along with these programs. Some universities either aren't capable of reaching the requirements or have the desire to. Have any of you heard of that issue before, any of that problem?

Ms. WORLEY. I have not.

Mr. KATKO. Dr. Estwick.

Ms. ESTWICK. So I would say there has been a little bit of a bottleneck in getting faculty members to teach in cybersecurity.

Mr. KATKO. Tell me about that. Why?

Ms. ESTWICK. We have been lucky enough to pull from private industry to have some adjunct faculty. But I would say, across the board—like computer science programs are having the same issues, actually. A lot of the companies—like she said, cybersecurities align and synergize a lot with the computer science programs.

So, for now, yes, I think this is where private industry and those, of course, coming from Government, can help step up and fill some of these faculty positions.

Mr. KATKO. So that—filling faculty positions will help us utilize a program we have now, because I think it is a terrific idea. I am not speaking for the Chairman, but I think he agrees—actually then, I am speaking for him. We both think that plussing up this program would be a very good place to start. We have to make sure that the universities are prepared to implement the program.

So, if there is changes that any of you think need to be done with the criteria so that we can make it more easy for these universities to get involved with these programs and get these kids these scholarships, please make sure you let us know, OK,

Ms. ESTWICK. Yes.

Mr. KATKO. Thank you very much.

Now, is it—we have had a lot of testimony from all of you today. I just want to hear kind of some spit-balling here.

What other ways that we can do other than what you have heard—you know, you have heard from Ms. Worley and the others. Is there something else, for example, Mr. Simpson or Mr. Gallot, that we can do to increase, at the college level, and get kids in? That is No. 1.

No. 2, if you want to add to it, do they always—do they have to have a college degree to do these programs? Because I think that they don't, and I would like to hear about that as well.

Mr. SIMPSON. That is an excellent question. Thank you very much for asking.

Let me first start for the first part of the question. I think if you are targeting college, you are too late. The majority of students choose their careers in high school. So in high school, we need to start sending that message of why cybersecurity is a great career, and why they need to get into it.

So when they go to college, if they choose to go to college, they can plan those curriculums and those degrees that align with that profession of cybersecurity that they want to get into.

Not all people go to college, though, so we understand that. That is the great relationship that academic colleges, as well as the certification and certificate organizations play, is that there is room for all of us, and that there is no one way to get into cybersecurity. There is multiple ways to get in.

People learn differently. There is nothing wrong with going through a hands-on technical program, certificate program, or certification program, or going through an advanced degree. It just depends on that individual. The most important thing is that they are going into cybersecurity and we help outline the different pathways and that journey map and that career map of how they can get into it.

Mr. KATKO. Now, the NSF scholarships, that applies strictly to universities, does it not? I mean, should it be expanded to apply also to certificate programs as a way of incentivizing kids to get into it?

Mr. SIMPSON. For us, absolutely. So when you look at how people are getting into cybersecurity, whether it is through certificates, certifications, or through education, scholarships play a huge path

for that. Especially for those folks that can't afford it. You start looking at some of these demographics in these areas, and then these individuals, they can't afford to go to college, they can't even afford some of these certifications.

The more we can infuse these programs of being able to cast a wider net and apply to a greater amount of students, that is how you are going to help with some of that inflow.

Mr. KATKO. Go ahead, Mr. Gallot.

Mr. GALLOT. Thank you, Mr. Katko, for that——

Mr. KATKO. By the way, I absolutely love your band at that university. Every time I see them on TV, I just stop what I am doing and watch. They just ooze talent, confidence, and fun. It is just a blast to watch them.

Mr. GALLOT. Thank you so much. We have a number of computer science graduates—computer science students in the band.

Mr. KATKO. I bet.

Mr. GALLOT. You know, quite honestly, you know, it is difficult enough for minority candidates in applying for jobs. For our graduates, I think, they are better prepared, both from a knowledge base, but also a maturity base, when they are going to either Government or the private sector applying for jobs.

So for a black student who is going and applying for a job, I think he or she stands a better chance of being seriously considered for that job if they have a degree. You know, that is part of the reality of the environment that we live in.

So, you know, certainly, I respect the fact that we have different entry points for different individuals. Ms. Worley, I think, did an excellent job of talking about the different needs that can be fit by some who have college degrees or not.

But our society now, I think, requires the students that I serve, they are much better prepared to go in and actually land that job with a degree as opposed to not having it.

Mr. KATKO. Thank you very much.

Last, I will just note, Mr. Chairman, perhaps we should consider when we are looking at the funding for the CyberCorps to make it more wide-spread for certificate schools, but also at the high school level, so kids who want to take college courses in high school might be able to have scholarship opportunities available for them. Then that gets them into the pipeline before they are out of high school.

I yield back.

Mr. RICHMOND. The gentleman from New York yields back. Now we will have the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank you for holding this hearing. I want to thank our witnesses for your testimony. You have all had important things to say about the cyber work force, something that I have been worried about for quite some time. This is an issue that I have been working on now for more than—more than a decade.

We often hear about the challenges in—in cyber and, you know, how does the, for example, the Federal Government compete and attract, and also retain people with the right cyber skills? I think that is the wrong focus to say how do we compete per se. It is really how do we grow the pie. So that is what we really need to focus on, so that we are not trying to compete or take from the private

sector, but again we are growing the size of the pie so there are more people available to fill these jobs that are necessary.

There are hundreds of thousands of cybersecurity jobs right now that go unfilled every year. That number is going to grow exponentially. We are probably looking into the millions several years out, as the cybersecurity challenges continue to grow.

So, you know, Mr. Simpson, I think you had some important things to say, too, about getting—how do we attract the kids at even younger ages and start thinking about a job in this field?

Certainly, I support the Scholarship for Service program. I led a letter to appropriators again this year asking for increased funding for the Scholarship for Service program. I think CyberCorps, it is a wonderful program, and anything we can do to grow or replicate those types of programs, we need to do that.

How do we create a program that talks to the—speaks to the kids at the high school level, so that they are thinking about that as a career? I think that we need a sort-of a—a program model so the Scholarship for Service program that we are—that we are reaching out to kids that are in college, right, now we can replicate that if we start talking to kids at the freshman, sophomore year, and saying the junior year, getting ready to go off to college, that you go into a cybersecurity field in a Scholarship for Service-type of program, your college in your—your freshman and sophomore year will be paid for, in a similar way, perhaps, that the junior and senior year will be paid for if you are in the Scholarship for Service program.

So have you thought about those types—how we can partner with the private sector and the Federal Government can go in that direction so that kids, as they are thinking about a career in cyber—or we get them thinking about a career in cyber, and they are starting to think about it in their high school years?

Mr. SIMPSON. Yes. Thank you for your question, sir.

It all starts with the awareness to the individual. So the kids today, they are not aware. When you look at the—the amount of, you know, Gen X and baby boomers that are about to retire over the next 5 to 10 years, there is not a wave of army that is coming over to help backfill them. So we have got to get into the school systems at a much earlier learning area to start to teach them. You have got to do that through investment.

Invest into the students, invest into the learnings, so on the back end, as they are going through middle school and high school, they are already aware, they have already got curriculum that has been put in there by the State into the schools. The broader that net that you can get across all of the—all of the schools within each State's district is going to start to yield that value as they transition, whether they go on to college, into a cyber career, whether it is through STEM or through STEAM or through certificates or certifications.

But bringing that technical, hands-on training, exposure at the high school level, is how you start to plant those seeds. It has got to be done through investment into those school systems and into the children.

Ms. WORLEY. Yes, I think there is—excuse me, Mr. Congressman. I think there is another opportunity, and that is, I think we

often forget that high school kids are probably as digitally savvy as most 4-year graduates were 10 or 15 years ago. I mean, they are digital natives. They can code at, you know, junior high, maybe earlier, in many cases. So there is probably opportunity where Government and private industry could partner together around internships at the high school level.

Often internships are something that is reserved for college, right? You get an internship once you get to college. We have got savvy high school students who are very capable, you know, from a cyber perspective. We should be looking at how we can partner together from a private and public perspective to create internship programs for those high school students.

You get them into a research facility with a bunch of cyber tech researchers, believe me they are going to get excited about this field, right?

I mean, you know, when they start looking at what they will get to do and the implications of that, we will get them excited. But I think there is an opportunity for us to partner that way.

Mr. LANGEVIN. I know my time as expired.

But, you know, you are right on point. When they can do more hands-on learning, I think that is the better—so I—I agree also with what you had to say. I hope you don't—it is not necessary that you need a Ph.D. right away to start going into the cyber field. We also need to include certification programs so that they can get the entry-level jobs in cybersecurity, even as they pursue other academic opportunities in either a junior college or a 4-year degree.

So thank you, Mr. Chairman. I could go on and on, but my time is gone. I will yield back.

Mr. RICHMOND. The gentleman from Rhode Island, Mr. Langevin, yields back.

The gentleman from Texas, Mr. Taylor, is recognized for 5 minutes.

Mr. TAYLOR. Thank you, Mr. Chairman.

I appreciate being here.

So just to kind-of expand on this. So as I understand the current program, it is for—it is at 68 4-year universities, so it is for a 4-year college degree, right? Is that basically how it works out?

So—and I just going back to saying we need more children to learn in high school. They need an associate's degree, maybe some community college, maybe some Ph.D. Is it a program that we should expand out in terms of, you know—you know, being thoughtful that, hey, sometimes it takes a Ph.D., sometimes it takes a college degree, sometimes it takes an associate's degree, sometimes it just takes a really sharp high school kid who has had 1 year of coding in high school so that we are looking at this in a kind-of a holistic level, because it is not just one entry point, like: Hey, this is the only thing you need. Like, we don't need any Ph.D.s or—am I thinking about that right, is it expanding this out?

Ms. Worley, since you are——

Mr. GALLOT. Congressman, I guess, part of what you—what I am here to talk about in terms of creating a diverse, you know, pipeline of cyber talent—and I think more globally, I think you make an excellent point. But specifically, what is it—what is that barrier that stands between this minority student and the cyber work

force, and how—how do we bridge that—that gap, which I think is the part that we have to—and if you look at, again, the students that we typically serve, many of them are still first generation college students.

Trust me, they—they find a way to figure it out. You know, not that everybody graduates from Morehouse and gets their student loans paid off. Some of our students, you know, actually work 3 jobs and figure out, like Jarrid Richards did, how to be an A and B student and get closer to that degree.

So I think part of it is resource and capacity to give us the opportunity to open this up to the students that—and the work force that I think the committee is here to talk about and address, and that is, how do we provide more access and resources, either through NSF or other agencies that you-all have that give us more capacity to provide access to the diversity that I think everyone is looking for?

Mr. TAYLOR. Ms. Worley, just going to you as an employer, right? So you are employing, you know, in my district, but also around the country, many thousands of people who are in this space. I mean, as we discussed before, I mean, you are hiring Ph.D.s and college graduates and associates—I mean, you have hiring all levels, right? Is that a fair statement?

Ms. WORLEY. In fact, there is a number of engineers in the office that I work in that do not have a college degree, but they are brilliant coders.

Mr. TAYLOR. Right.

Ms. WORLEY. So, you know, I fundamentally believe in education. I worked my way through college as well. I paid for both my undergraduate and graduate degree, you know, cocktail waitressing, waitressing, cooking, whatever it took. So I understand that 4-year degree and the importance of that.

But there is also a population in our work force today that maybe has, you know, 20 years of experience in a job doing data analysis, but they have never worked in cybersecurity. But believe me, that data analysis experience they have would be outstanding as an incident responder in a cybersecurity operations center.

We need to look at the requirements, not just the hard-coded requirements of working in cybersecurity. What are the skill sets we need—critical thinking, problem-solving analytics that apply? And then create programs, whether those are through certification programs, vocational programs, a community college program that allow them to take the skills they already have and translate them into the language of cybersecurity. That doesn't necessarily take the 4-year degree.

If I am fresh out of high school, that 4-year degree probably is going to be really important. If I am an experienced person, maybe less important.

Mr. TAYLOR. Sure. I know in my own State of Texas, we are at about 24 percent of our population has a 4-year college degree. We are trying to get to the National average, which is 27 percent. In that effort, we are actually not leaving anybody behind. We are actually—we have implemented a 60/30 plan to try to get 60 percent of the population by 2030 to have some kind of post-high school de-

gree or certification, right? Whether it is a welding certificate or an associate's degree or a 4-year college degree.

But it seems in this space, the requirements are such that if you focus only on the college degree, you are missing key pieces under and below that you have got to have in order to have an effective work force.

Ms. WORLEY. Furthermore, given where we stand right now, if we rely solely on 4-year degrees, we will never catch up. We have to look at creative ways to educate people with experience, to educate people with core capabilities in this space, and we still need lots of college graduates. There is no doubt of that, because if you start looking at things like data science around artificial intelligence, that requires education. But we should not bypass a lot of those other individuals that have core capabilities relevant to this field because they simply don't have a degree. We should enable them to move forward into the field.

Mr. TAYLOR. Right. I should point out that an associate's degree could be on the way to getting a college degree, right? So you encourage somebody to get an associate's degree, they work for a couple of years, and they say, you know what? I am going to go back, and I am going to finish up my bachelor's degree.

Ms. WORLEY. Absolutely.

Mr. TAYLOR. I am out of time. Mr. Chair, I yield back.

Mr. RICHMOND. The gentleman from Texas, Mr. Taylor, yields back.

The gentlewoman from New York, Miss Rice, is recognized for 5 minutes.

Miss RICE. Thank you so much, Mr. Chairman.

You know, what I am hearing here today is very encouraging. I think that what I would love for the Chairman and the Ranking Member on this committee to do is to put together all of these parts, right? We have educators, we have the private sector who needs to employ people, and we have Government that has a vested interest in educating and training a work force for the future.

I think people fall into two categories: You have those heading into college or who are already in college. I was just at my nephew's graduation at Catholic University, my alma mater. I said, Thank God he went into business, because maybe he has a chance of getting a job when he graduates. So we have that whole universe. How do we get qualified teachers at the high school level? Maybe—I am just going to throw a bunch of questions out, and whomever thinks they can answer them, answer them.

But we need to have faculty in high schools, grammar schools and high schools, that are up-to-date on IT issues and cyber issues, so we can get kids interested at a high school level. You know—and I think that is where you increase the chances of diversity going forward.

But we also have a large number of people in this country who got a degree that maybe cannot help them get a job. I mean, every time you talk to people who are based in Silicon Valley, they say we have millions of jobs that we cannot fill because we do not have a trained work force in this country.

So do we partner together—there are three legs to this stool. We need educators, we need the Government, and we need private

business. Everyone has a vested interest in coming up with a system that will work.

Now, the reason why I think it is important to go in at a high school level is because there is still out there that sentiment that I need to get a 4-year degree. No offense to anyone who heads universities that offer 4-year degrees. That is not true. Maybe an associate's degree is OK; maybe you just need to go to vocational training. But there still seems to me to be somewhat of a stigma, right, around not going and getting a 4-year degree, when we have all of these kids who are graduating with crushing student loans that is ultimately going to become the taxpayer problem, right?

So here is one question: How do we ensure that we get a faculty in high school who can actually begin to get these young kids interested in these sciences, technologies, AI, whatever it is, and how do we address the issue of there being a stigma to maybe just going and getting vocational—a vocational education that, by the way now, you can end up making more money than someone who graduates with a 4-year degree?

So it is just a lot of stream of consciousness. But, literally, I was just sitting with my nephew and I thought: Thank God he has a job. But there are—how many of his classmates don't and they have got these crushing student loans.

So anyone who has any thoughts on that?

Ms. ESTWICK. Congresswoman, thank you for those questions. I really would like to jump in and say this, because I feel passionately just like you about our educators.

Educators are our force multipliers, right? What we are doing is, I feel like we are teaching our students, like, who are digitally natives, right—digital natives, and they are surpassing the teachers. We have communities where—you may not know this, but the teachers share a—a lot of the educators shares this—you know, students are going in and changing their grades, because they know how to hack the systems and they know how to compromise weaknesses, right, in the network.

So they already have that capacity and that intellectual curiosity, where our educators are sitting there trying to keep up. So I think programs that are focused around trying to help our educators so they can feel empowered to then be a force multiplier and explain cybersecurity jobs, not in the form of the cool stuff they see in Hollywood and hacking, right, but also things to protect our National security, right?

Miss RICE. What is the biggest obstacle to getting that work force that is ahead of young kids that, you know, as you say, are better than any of us?

Ms. ESTWICK. Absolutely, absolutely. So I think there are programs—and I can't stress this enough, because GenCyber is such a major program that I don't think it gets funded enough, to tell you the truth. This is a National program that has been around for about 5 or 6 years, and they host camps, cybersecurity camps, and they teach the fundamentals. They come out of the—the budget comes out of, I believe, National Security Agency, National Science Foundation.

But what it is, is that about 130 camps were awarded this year. The camps are there—they have teacher camps, student camps,

and a combination sometimes of teachers and students. So you have kind-of train-the-trainer effect.

So last year when we hosted—Excelsior College, we hosted and was awarded a grant to host a middle and high school cybersecurity camp. We provided them with tools, many computers—we called them raspberry pies. We taught them lessons. So now they are taking that—and our teachers were diverse. They weren't just, you know, our comp sci or our biology or our STEM teachers. We have librarians, because they are now the house—they are the custodians of the technology, sometimes in the high schools and the schools.

So we have librarians, we have our technical teachers who do the vocational training, and we had various disciplines in the camp, about 30 educators in there. Just teaching them and providing them with the curricula so they are able to, again, then train their teachers and then that kind-of replicates throughout the system. But naturally, these programs need to be supported to expand.

Miss RICE. Uh-huh.

Mr. GALLOT. I would like to add, we have, at Grambling, several summer programs. We have one high-ability program for rising juniors. So they come to the campus, essentially are college students for the summer program. We could have 10 times of number of students that we have, if we had the resources to fund that program.

We also have computer camps. We have STEM camps. We are joining a partnership with Dr. Calvin Mackie from New Orleans, which is STEM NOLA, where we are making it STEM Grambling.

There are a lot of—we have the ability to do a lot more if we had resources. I would say that, you know, what Mr. Walker and Senator Scott are doing every year with HBCU Fly in, it gives HBCU presidents a platform to interact with agency heads, with—with industry at the request of Members of Congress.

So using your platform to connect us with the resources, both at your respective agencies that you oversee, as well as the businesses that are always looking to have a relationship with you to put them in the room with us.

So, I thank Mr. Walker and Senator Scott for what they have done for the past 3 years in giving us a forum to develop these relationships. We see greater capacity, but we could do even more if we had greater resources.

Miss RICE. Well, it is clear that all of us are aware in this room that we are all in this together, and I think we just need to kind-of get in the same room and figure out how we do this.

So thank you all.

I yield back. Thank you, Mr. Chairman.

Mr. RICHMOND. I thank the gentlewoman from New York.

I now recognize the gentleman from North Carolina, Mr. Walker.

Mr. WALKER. Thank you, Mr. Chairman. Thank you, President Gallot, for those kind words. It was great to see you again this past February. Of course, I won't talk any North Carolina A&T shade, although obviously I get to represent the great university. As you know, my wife went to Winston-Salem State University, so that whole Aggie Pride Ram. I can tell Mr. Morehouse is over there looking down at me already. But we will leave that alone for today.

But I do appreciate your commitment in helping these young students to exceed in all aspects of life.

I read through a little bit of your testimony. It is apparent that Grambling State is becoming a leader—already a leader, and even expanding that in cybersecurity education efforts.

Can you describe how Grambling State began its partnership with the IT companies?

Mr. GALLOT. Graduating qualified members of the work force. I think, you know, showing that we are graduating not only 40 percent of the African-American graduates in the State of Louisiana in computer science and CIS, but those who can actually come in on Day 1 and make a difference. Even with our interns—and I highlighted earlier, one of our students who did an internship at an electrical utility who came in, and his supervisors complimented him on being prepared to come in and do meaningful work as an intern, as opposed to just, you know, fetching coffee or doing something menial.

So, I think the quality of our graduates is what has opened the doors to many of the relationships that we currently have.

Mr. WALKER. I don't want to be too technical. If it is, take a pass on this. But I would like to kind-of dig a little deeper. Can you describe the difference between a cybersecurity course versus a computer science course?

Mr. GALLOT. I defer. I could—I could read the curriculum. Of course, there are foundations of cybersecurity.

Mr. WALKER. Sure.

Mr. GALLOT. There is the technical aspect of it of the what to do, but there is also the why. So there is the ethics around it all——

Mr. WALKER. Exactly.

Mr. GALLOT [continuing]. Of course. So that is a part—it is a holistic approach that we are taking with our new program. But I would certainly defer to——

Mr. WALKER. Well, and I would have to as well. I get to read the questions sometimes with the good staff work, just to be honest with you here, on some of the dig the thing out, if I can be honest with you here for a second.

Let me do a follow-up. Maybe this helps. A 2016 study showed that only 1 of the top 36 computer science programs required any cybersecurity course to graduate.

Do you think that more schools—and I will open this up—I won't pick on President Gallot—do you think that more schools should include cybersecurity components in these computer science programs?

Mr. SIMPSON. So I will jump in here real quick. So I actually think it should be part of—it should go further beyond computer science. I think it should be part of Common Core.

When we look at cybersecurity, this is an epidemic issue that we are going through globally. If we don't start getting out the education awareness and building this into our school systems, it is just going to continue to grow.

Typically, we just go after the STEM candidates, the science, the technology, as well as engineering and math. We need to go broader than that. We need to really get into the STEM—STEAM, which brings in the arts.

Cybersecurity should be part of, at least, a course in all degrees, because when we look at how we are going to solve this, especially in the workplace, it is not just the cybersecurity team; it is everybody. It is all of the employees need to know what their hand is in this and how they are going to be able to help.

Mr. WALKER. Ms. Worley, go ahead.

Ms. WORLEY. May I?

Mr. WALKER. Yes, of course.

Ms. WORLEY. Thank you, Congressman.

So I think it absolutely has to be part of the core curriculum—I agree with Mr. Simpson—in that as we contemplate the internet of things and the continued digitization of everything that we live with in our world today, enabling students who are going to be designing—whether that is designing software or designing hardware, et cetera, to be designing with security in mind from the beginning, from architecture and development, is absolutely critical to the security of everything that we use at home, in our companies, and in Government.

Enabling them with the basic tenets of cybersecurity, whether they are going to be software coder or a hardware developer or a cybersecurity expert is absolutely fundamental to ensuring kind-of a secure digital ecosystem as we move forward.

Mr. WALKER. I am glad to hear that.

As Ranking Member on counterintelligence and terrorism on this specific subcommittee on Homeland Security, I can tell you, the Chinese try to hit us 20,000 times a day, Russia as well. We need strong young people that are coming into this environment that can speak this language, for lack of better expression there. I think that is crucial.

One survey found that only 37 percent of students said that a teacher discussed with them cybersecurity as a career option, with a contributing factor possibly being the lack of skilled teachers.

How do you change that factor? Because you can only educate for people that you have to—from the educators down to the students.

Somebody want to address that? My time is expiring with that question.

Dr. Estwick, you want to take a look at that?

Ms. ESTWICK. Right. So thank you for that question, Congressman.

So you are talking about, as far as how do we get cybersecurity and computer science in conjunction and also, how do we get teachers? I think—educators, right?

So I think the thing is that there is work that is being done. Looking at the Common Core standards—we talk about this all the time, about the standardization, right, and looking at how we are already infusing computer science into the curricula, as well as synergies between that and, you know, infusing the cybersecurity components.

But I have to tell you, sir, without question, we are playing catch-up, right? So we have educators who are trying to wrap their heads around the standards as it is, and then we have a hodgepodge of standards, as you know, Nationally, right? So some States are a little bit more mature than others.

When you look at the standards—I am going to reach out there and say, like, New York—because our school is based in New York, so I know a little bit about their standards, and I am on the K–12 subgroup through NIST, actually, that is trying to synergize between computer science and cybersecurity. You will see that there is a lot of commonality. But you will also see that those tenets that we talked about that is part of cybersecurity, educators need to be educated on that as well. So it is not just a curricula for the students. It is also a curricula for the educators who are trying to be the force multipliers in the classroom.

Mr. WALKER. Thank you.

Mr. Chairman, I yield back.

Mr. RICHMOND. The gentleman from North Carolina yields back.

I will recognize myself for a round of questions.

Let me go back and just start kind of at the basic. I will start with you, Dr. Estwick.

Based on your experience in the Army, National Security Agency, now academia, how important is it for Federal agencies, National security agencies, intelligence agencies with those missions, like DHS, FBI, DOD, to have a diverse cyber work force?

So, I guess the ultimate question is, do you think that having a lack of a diverse work force actually creates inherent blind spots in our security?

Ms. ESTWICK. Well, thank you, Mr. Chairman, for that question.

I feel that, you know, there has been—already studies out that—the importance of diversity in the work force. Especially, I would feel in the cybersecurity and in the National security framework, diverse perspectives are important.

For my experience, I feel that there is certain ways—experiences I bring to the table that other people just don't have. Having a multitude of people around you with all of those different perspectives will—we are able to see different areas of a problem.

I think for me working 10 years in cyber operations, there were different avenues that I was able to identify ways that maybe we, you know, can get ahead of the adversary and not be so prone to always be on the defensive side and playing whack-a-mole, frankly, when we are trying to protect our resources.

So I think it is important that we—diversity, we know, is a business problem, right? We know diversity needs to be focused and brought to the table. But I think it is also that we talk about diversity a lot in conversations. It is a little frustrating for me sometimes, because we talk a lot about it, but I don't see it in action, unfortunately.

What that means is there needs to be some entrenched—there is entrenched issues that need to be addressed. Some of that could be not just mentoring, but also with sponsorships. So how do we bring people through the different grade levels so they are able to be a part of problem sets and be a part of the overall solutions to how do we address diversity and, again, protect our National security.

Mr. RICHMOND. Thank you.

Let me ask Mr. Gallot. We have talked about the CyberCorps Scholarship for Service, which it appears that everybody up here supports.

I would assume, Ms. Worley, you would tell me that if we doubled it, you think everybody would use the money and continue to create more of a pipeline. But besides the CyberCorps Scholarship for Service, what about programs like DHS or NSA Centers for Academic Excellence, how can they better partner with you? How can—what else should we be asking them to do to help create that diverse pipeline, maybe partnering with HBCUs or other minority-serving institutions?

Mr. GALLOT. Well, I think part of the solution is providing additional support resources. I am not just talking about writing a check. But when you think about our shop, for instance, our sponsored program director, Dr. Walton, is also serving as our provost. So her ability and time to—although she has increased our research grants by 254 percent in the last 2 years, there is so much more that could be done if there were more of—more workers in her shop to help us connect with those resources.

So having an agency like—like DHS to provide a resource person to connect us with that—with those opportunities, I think, is something tangible that would assist us. Again, it is not about just writing a check; it is about giving us some help to build our capacity to compete for these opportunities.

Mr. RICHMOND. Well, I am glad you brought up the professor. I think about people like Calvin Mackie, STEM NOLA, and you all partnering.

The question is, how long will we keep them in the public service sector before the corporations who need people, who have deeper pockets, come along?

So, I mean, how hard is it to retain department chairs and professors? Because if you are talking about a 489,000-person shortage in the country, at some point they are going to start picking off our professors to start working in the high-paying jobs. Then all of a sudden, who is training the next generation? So do you see a problem with retaining and recruitment?

Dr. Estwick, you also.

But do you-all see a problem in the future of retaining the talent that is teaching the next generation of cybersecurity talent, and how can we help you all keep them in academia as opposed to going off into the private sector by Ms. Worley and making a whole lot of money?

Mr. GALLOT. Mr. Chairman, I think if you all as Congress can incentivize the private sector to better partner with us, I think would certainly be a good start. They certainly want to know how they can continue to do business with you. If their contracting documents require a certain level of partnership with academia, I think that incentivizes them to be a better partner with us, because you are requiring them to do it as a part of doing business with you. Does that make sense?

Mr. RICHMOND. I understand what you are saying.

Dr. Estwick.

Ms. ESTWICK. Yes. I can also—thank you, Chairman, for the question.

I can also add that I think in the Executive Order, they spoke about rotational assignments. I think it is important to have kind-of that cross-pollination, right? So you have folks—and, again, it

incentivizes the program. But being able to have private industry go into Government, Government go into private industry, academia, and just have this continuous cross-pollination of information, of experiences, of expertise, I think would be important, too.

So when we talk about this in the framework of the Executive Order and the rotational assignments, I would like to see that really expanded to include not just the Government, but also with private industry and the academic communities as well.

Mr. RICHMOND. I see that my time has expired. So I will yield back.

Before I close the hearing, I will recognize Mr. Katko for additional time.

Mr. KATKO. There is no question. I just want to make a brief observation, based on all of the excellent questions and input from the panel today. That is my experience with a program called P-Tech in high schools. I am not sure many of you have heard of it, but what it does, it has kind-of come out of an outgrowth of a need in the STEM fields, electrical engineering and all of those types of things. But also in some of the rural areas, it is a way of getting people into the building trades.

What they do is they marry up the industry with the kids in high school in an earlier level, 8th, 9th grade, and they get them in the college-type—college-level courses, but also give them practical experience. They are being taught oftentimes, at least at a guest lecture, and sometimes in the classroom setting, by members from the industry.

So, by the time they get out of high school, they have a lot of college credits, they have a career goal, and they know what they are doing. Oftentimes these are first-generation kids going to college. It is working everywhere it goes.

So all of the talent in the industry—you want to talk, Mr. Gallot, about bridging the gap, right, and having Government help augment things. Industry can augment Government by getting their people out into the field and reaching to these kids at these early levels in a P-Tech type program. You could do that all over the country, and I think would have a huge effect as well. Then you couple that up with the scholarships—and us plussing-up the scholarships, you might really start having a force multiplier that we haven't seen before.

But getting industry not just looking for talent, getting them out into the field to help cultivate that talent would be a very big thing.

With that, Mr. Chairman, I yield back.

Mr. RICHMOND. I ask unanimous concept to submit a statement for the record from New America.

Hearing no objections, so ordered.

[The information follows:]

STATEMENT OF LAURA BATE, POLICY ANALYST, NEW AMERICA

MAY 21, 2019

Chairman Richmond, Ranking Member Katko, Members of the subcommittee, thank you for the opportunity to provide written testimony for today's hearing on "Growing and Diversifying the Cyber Talent Pipeline." The Members of this subcommittee undoubtedly understand the critical importance of effective cybersecurity.

Protecting data and information systems throughout the Federal Government and military is fundamental to protecting National security, but our considerations must extend beyond that.

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

I work with partners in higher education, private industry, and public service to improve our understanding of the dynamics that shape the cybersecurity workforce. As a policy analyst with the Cybersecurity Initiative at the think tank New America, my research encompasses both how we expand that workforce and how we strengthen it through diverse perspectives and educational pathways that evolve to meet the challenges of cybersecurity's changing landscape.

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

DIVERSITY IS A FEATURE OF STRONG CYBERSECURITY TEAMS

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

1. Inadvertently limiting diversity artificially narrows hiring pipelines. We cannot afford to overlook entire demographics when we consider the pool of available talent. The United States needs to fill more than 300,000 cybersecurity jobs. There are an estimated 715,715 workers currently employed in cybersecurity jobs,[2] which means that the industry must grow by more than 40 percent just to meet current needs, let alone future requirements. Given the scale of the demand and the importance of these jobs, the country is best served by prioritizing the identification and removal of the barriers that discourage diversity in the cybersecurity industry.
2. Diversity makes teams stronger. Research indicates that diverse teams focus more on facts, process those facts more carefully, and are more innovative.[3] Because we are discussing the teams that will protect Americans' lives and livelihoods, we cannot afford to field anything less than the best teams possible.
3. Cybersecurity jobs pay well. Ensuring that these economic opportunities are equally accessible to all members of our communities is simply the right thing to do.

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

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

---

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

[2] *Cybersecurity Supply/Demand Heat Map.* CyberSeek. *https://www.cyberseek.org/heatmap.html.* (Accessed May 2019).

[3] Rock, David and Heidi Grant. *Why Diverse Teams are Smarter.* Harvard Business Review, November 4, 2016. *https://hbr.org/2016/11/why-diverse-teams-are-smarter.* (Accessed May 2019).

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

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

INNOVATION RESPONDS TO INCENTIVES

Growth in the cybersecurity workforce is hampered by limited opportunities for potential employees to enter the field and gain experience. The most commonly requested professional certification,[4] the CISSP, is not granted in full until candidates can demonstrate 5 years of relevant work experience.[5] Notably, in the United States there are currently more job postings seeking candidates with this certification than there are certification holders throughout the whole of the economy.[6] The large majority of open cybersecurity jobs require several years' experience in the field and a minimum of a bachelor's degree.[7] [8] The cumulative effect of these requirements for degrees, certifications, and experience is that it can be quite difficult to find that first job in cybersecurity, especially for job seekers without a degree in computer science or a related field.

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

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

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

With careful implementation, workers, employers, and educators all stand to benefit from more widespread adoption of cybersecurity apprenticeships.[11] Simply spreading the model, however, is not enough; quality matters in apprenticeship programs. In order for the cybersecurity community to benefit from apprenticeship pro-

---

[4] *Cybersecurity Supply/Demand Heat Map.* CyberSeek.

[5] *CISSP—The World's Premier Cybersecurity Certification.* (ISC)². *https://www.isc2.org/Certifications/CISSP.* (Accessed May 2019).

[6] *Cybersecurity Supply/Demand Heat Map.* CyberSeek.

[7] *Job Market Intelligence: Cybersecurity Jobs, 2015.* Burning Glass, 2015. *https://www.burning-glass.com/research-project/cybersecurity/.* (Accessed May 2019).

[8] *Cybersecurity Supply/Demand Heat Map.* CyberSeek.

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

[10] *State of Cybersecurity 2019: Current Trends in Workforce Development.* ISACA, 2019. *http://www.isaca.org/cyber/Documents/State-of-cybersecurity_res_eng_0316.pdf.* (Accessed May 2019).

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

grams in a sustainable way, measures to expand apprenticeships should support programs that ensure four basic features, drawn from the Apprenticeship Forward Collaborative:

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

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

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

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

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

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

GOOD DATA IS SCARCE

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

For example, it is difficult to know which pathways brought current cybersecurity workers to their present positions. Anecdotal evidence would suggest the military, intelligence community, self-taught instruction, and conventional 4-year degrees are all major contributors, but we have very little means to judge those in relation to one another or to identify other major pathways. Similarly, we have very little longi-

---

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

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

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

tudinal data from employees in cybersecurity fields to identify which pathways lead to best outcomes for learners over the course of their career.

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

Cybersecurity workforce development is receiving an unprecedented amount of attention from the highest levels of Government and industry, and yet we still cannot authoritatively and consistently answer even very basic questions about the current workforce: What percent of the U.S. cybersecurity workforce is female? How many cybersecurity professionals does the U.S. Government employ? What makes a cybersecurity employee—in any role—effective? When these questions are answered at all, the answers vary significantly depending on whom you ask, and the field is rife with studies with inconsistent methodologies and unacceptably small and biased samples.

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

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

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

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

Mr. RICHMOND. We are trying to give one of our colleagues a moment to get here, and I think that she would add valuable insight into the conversation.

But let me just also add that we really need to find better ways to fund, especially our CyberCorps scholarship program. The fact that I believe every year in the budget, it is identified as something that would and should be cut. I am sure that it is very hard to—to have a strategic plan if you don't know if that funding is going to be there on a yearly basis. Maybe we ought to look at some long-term funding for it or making sure that we know it is there so that you can plan accordingly.

Now, Mr. Gallot, I guess when I was coming up in high school, we had Upward Bound and all of those programs where kids could go to college and get introduced to biology and all of those pre-med—not that I got into any of the Upward Bound programs, but I certainly knew that they were there.

So is that what you-all are doing in terms of cyber and computer information systems? At what grade do you start?

Mr. GALLOT. So those—we don't have TRIO or Upward Bound. Southern University, of course, in Baton Rouge has that. Ours are self-supported programs. Our high-ability program, again, for rising juniors who are able to come and earn college credit on a college campus, as well as our—we have coding camp. We have a robotics camp.

Mr. RICHMOND. How do you pay for all of that?

Mr. GALLOT. Mainly, we absorb the cost or through some grant opportunities. But for the most part, we absorb the cost. Because, again, a lot of students we serve lack the resources to—to pay for that. Of course, with our—our partnership with Dr. Mackie and STEM Grambling, that is going to provide us additional opportunities. Entergy, for instance, has been a great partner of his program, and so, we look to utilize those as well.

But again, we have the ability and the know-how to do it. It is just simply a matter of having expanded resources to expand our capacity to reach these kids who are really very hungry, and they are like sponges. I mean, they soak it up very, very quickly. You just have to give them an environment to do it.

I think about my 6- and 7-year-olds who are using iPads in Kindergarten and 1st grade. So these kids growing up now are, you know, way more technologically advanced than we ever were, and they pick up on this stuff.

Again, we just need more capacity and resources, and we can certainly do a better——

Mr. RICHMOND. Now, are there any Government programs or grants out there for the universities to help you augment or offset those costs for those programs? Or is that something you would like to see us look at creating?

Mr. GALLOT. We would certainly welcome the opportunity.

Mr. RICHMOND. OK. With that, I want to thank the witnesses for their valuable testimony and the Members for their questions.

The Members of the committee may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to those questions.

Without objection, the committee record shall be kept open for 10 days.

Hearing no further business, the committee stands adjourned.

Thank you.

[Whereupon, at 4:13 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE LAUREN UNDERWOOD FOR AMELIA ESTWICK

Question 1a. Right now, there are 300,000 unfilled cybersecurity jobs in this country. For the sake of our National security and our international competitiveness, that needs to change.

Fermi National Lab, in my District, is working to make that change by bolstering the cybersecurity pipeline for veterans through their innovative VetTech internship program. These paid internships provide training in computing, software development, and electrical engineering, providing the skills needed to enter the cyber workforce. This past year, the VetTech program received more than 50 applications for 12 openings.

As a veteran yourself, can you tell us more about why targeted, Federally-supported programs like VetTech are so important for widening the cyber workforce pipeline?

Answer. Programs such as the Fermi National Lab VetTech's internship program are so important for widening the cyber workforce pipeline because this program and other internship programs tap into a resource of highly-skilled individuals who may already possess some of the technical competencies to work in the cyber workforce, to include, critical analysis and engineering, as well as soft skills such as leadership, communications, and business acumen. Internships (both virtual and in-person) provide opportunities for veterans to work within the contexts of corporate culture which oftentimes is different from their military work culture. As part of these programs, they acquire first-hand experiences with the cyber issues facing business, Government, and nonprofits. This is particularly important for individuals looking to change their career to take advantage of opportunities in cybersecurity. At Excelsior College, our student demographic is 30 percent military/veteran and we have worked on developing an option for students to complete an internship for credit. By participating in internships, students gain practical work experience that they can use to demonstrate their skills and potential to future employers. For employers hosting interns, there is a potential to increase capacity in the short term and build talent pipelines in the long term.

Question 1b. In addition, your statement, "the VetTech program received more than 50 applications for 12 openings", speaks to the need and desire of veteran programs such as VetTech that cater and support their career transition.

What are best practices that institutions of higher education and technical education programs can implement to attract more veteran applicants?

Answer. Some of the best practices higher education institutions and technical education programs can implement to attract more veteran applicants are to provide as many opportunities to aid veterans in their career pathways. For higher education, this means support for veterans in acquiring their academic credentials by offering flexible options for them to use their GI Bills (to include the original GI Bill of 1944 and Post–9/11 Veterans Educational Assistance Act of 2008), landmark pieces of legislation that have helped millions of veterans pay for post-secondary education. Providing flexible options which include virtual and in-person, would benefit the veteran especially if they are currently working and need the academic credential or vocational training to advance in their career path.

In addition, according to the Association of American Colleges and Universities, it's imperative to have effective programmatic elements to meet veterans' unique needs, which may include collaboration with other community support services to ensure successful transition and matriculation throughout college. For example, Excelsior College established the Center for Military and Veteran Education (CME), which offers supportive services to service members and veterans, such as:

"Provide specific points-of-contact to aid in higher education governance. For many veterans, higher education can be a culture shock in understanding the institutional governance; therefore, the CME provides specific points-of-contact for all services

(e.g. registrar, academic advisement, tuition assistance, career services, etc.) to alleviate veteran student frustrations.

"Create veteran-specific learning communities. Excelsior College's student demographic is 30 percent service member and veteran; therefore, creating learning communities that focus on this student population (e.g. social media groups, etc.) has benefited many of our service members and veterans by enhancing their student experiences and fostering a supportive network of peers."

Finally, educational programs that emphasize internships, apprenticeships, externships, and mentor/protégé programs that will assist in guiding veteran applicants during their career transition, can be used to attract veteran applicants. These experiences help to reinforce skills learned and provide veterans with practical experiences that can help shape their career pathway.

Question 1c. What could Congress and the Federal Government do to help make veterans more aware of opportunities within the cybersecurity field?

Answer. Initiatives Congress and the Federal Government can implement to make veterans more aware of opportunities within the cybersecurity field are supporting outreach and workforce development programs that reach veterans. Outreach in the form of marketing campaigns targeting veterans for cybersecurity jobs, such as social media, advertisements on public transportation, radio, as well as strategic partnering with the U.S. Department of Veterans Affairs and Department of Defense; leverage the existing platforms and services currently used by veterans. Also, there should be an emphasis on sponsoring National job fairs for veterans as well as collaborating with private organizations to incentivize veteran recruitment, and continue funding for free cybersecurity training for veterans, such as the Federal Virtual Training Environment (FedVTE). Finally, using cybersecurity professional organizations such as Women in Cybersecurity (WiCyS) and International Consortium of Minority Cybersecurity Professionals (ICMCP), that target affinity groups such as veterans and other diverse populations, are another great resource to bring awareness to veterans about opportunities within the cybersecurity field.

Question 2a. Even with VetTech's success in attracting applicants, I've heard from stakeholders in my district that further engagement with community colleges and 4-year universities is also necessary for cybersecurity training programs to be sustainable.

Dr. Estwick, what support do colleges and universities need from Congress to fill the growing demand in the cybersecurity workforce?

Answer. Public and Private partnerships are paramount to growing the cybersecurity workforce. Cooperation of private industry, academia, and Governmental agencies on joint cybersecurity initiatives can take advantage of each sector's complementary strengths. For example, in 2014 the Office of Personnel Management (OPM) created the Federal Academic Alliance (FAA) to provide higher-education opportunities to the Federal workforce at reduced tuition rates to address the Government-wide skills gap needs, including the shortages in cybersecurity. Today, OPM endorses 15 colleges and universities, such as Excelsior College and support for more educational opportunities like the FAA would be beneficial to fulfill the demand in the cybersecurity workforce.

In addition, according to a recent International Information System Security Certification Consortium, (ISC)² 2018 study titled, "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," 26 percent of the U.S. cybersecurity workforce identifies as non-Caucasian. One strategy to address the underrepresentation of racial and ethnic minorities in the cybersecurity field is to fund cybersecurity educational programs at minority-serving institutions (MSI). More funding for MSI's to create cybersecurity educational curricula that addresses cybersecurity topics (e.g. data breaches, threats to internet of things (IoT), artificial intelligence (AI) expansion, etc.) would help to educate and sustain the cybersecurity workforce while broadening participation within the cybersecurity field.

Finally, the number of cyber attacks targeting our Nation's critical infrastructures are on the rise. Specifically, in 2013, 59 percent of the attacks against our critical infrastructure were reported in the energy sector (ICS–CERT, 2013). A skilled and educated workforce is an essential component in improving the security posture of our critical infrastructure. The security program of the nuclear sector is regulated by the Federal Government with governance under the U.S Nuclear Regulatory Commission (NRC). In addition to being competent in cybersecurity, professionals working in the nuclear and energy industries need to be aware of specific standards, requirements, and unique cyber threats.

Excelsior College has a long history of meeting the educational needs of the nuclear workforce through innovative educational solutions. In 2014, a degree program was created to address cybersecurity challenges facing the nuclear industry. Cyber-

security professionals in the nuclear sector require a broad range of technical skills; however, few college programs currently exist at the baccalaureate level to assure that these professionals have the unique skill sets and knowledge domains needed to protect facilities and our National security. Additionally, the critical and practical nature of nuclear and energy sectors calls for enhanced simulation-based learning to be developed. Due to Excelsior's innovative program, in June 2018, Excelsior College received a Department of Energy Nuclear Energy University Programs (DOE–NEUP) grant to purchase a web-based pressurized water reactor simulator for use in the nuclear engineering technology program. The ~$250K grant provides funding to:

- support plant simulation to enhance student achievement of higher cognitive learning outcomes through "learning by doing,"
- provide the ability to evaluate and analyze technical information during "dynamic" situations,
- enhance our student's experiential learning activities, and by doing so, enhance the student's ability to meet industry needs,
- enable students to advance their understanding of key theories and concepts in the nuclear technology field to better protect against cyber threats.

The value of Government funding to support the development of these lab-based activities means without such support, higher education institutions might not be able to adopt this important technology. Therefore, there is an increasing need to expand Government funding of experiential learning, especially in an on-line environment, where skills shortages in cybersecurity can be filled by shifting people from one industry/occupation to cybersecurity fields.

Question 2b. As both a veteran and woman of color, what do you believe are the most impactful barriers to entry that need to be addressed to attract and retain these underrepresented groups?

Answer. As a veteran and woman of color, some of the challenges to recruitment and retention within the cybersecurity workforce have and continue to be: Lack of understanding of military transferable skills, discrimination, and inequities with pay and access to career opportunities.

Female veterans need more support in articulating their military experiences and identifying transferrable skills important to the cybersecurity domain. Since there's no direct mapping of military careers to current cybersecurity jobs, the lack of understanding by many employers when it comes to hiring veterans gets further complicated when the veteran is unable to articulate the importance of their military jobs. Therefore, employers need to implement recruitment programs with hiring managers who understand the immeasurable value female veterans bring to the cybersecurity workforce.

According to a recent 2017 Global Information Security Workforce Study, 51 percent of women in the cybersecurity workforce have experienced discrimination. Although this statistic did not disaggregate how many were female veterans or women of color, we can surmise these female populations face discrimination as well. To further support these statistics, the (ISC)^2 2018 report referenced in an earlier question stated "32 percent of cybersecurity professionals of color report they have experienced some form of discrimination in the workplace." Awareness programs that address diversity, inclusion, and equity are important for organizations to recruit and retain veterans and women of color in the cybersecurity workforce.

Finally, from my personal experience, it's important that we continue mentorship programs; however, sponsorship programs have directly impacted my career advancement. Sponsors take a direct role in the advancement of their protégés and usually work within the same organization. It was through sponsorship and endorsement of my technical competencies by senior leaders that advanced my career from a multitude of roles that garnered more responsibility at each level, while affording me the opportunities to earn raises and promotions along the way. Without sponsorship, my cybersecurity career path would have likely stalled in non-managerial roles negatively impacting my pay and access to technical leadership programs. Unfortunately, the inequity issues with pay and access are not unique; according to the (ISC)^2 2018 report referenced in an earlier question:

"Despite higher level of education, a cybersecurity professional of color earns less and is underrepresented in senior roles . . . tend to hold non-managerial positions, and pay discrepancies, especially for minority women (whereas women of color make an average of $10K less than Caucasian males and $6K less than Caucasian females)."

In conclusion, there are several barriers impacting veterans and women of color in the cybersecurity field; however, based on my experiences; the inability to articulate transferrable skills, the lack of pay equity and access to career opportunities

due to discrimination would need to be addressed to recruit and retain veterans and especially women of color within the cybersecurity field.

Sources: *https://cme.excelsior.edu/, https://fedvte.usalearning.gov/, https://www.wicys.org/, https://www.icmcp.org/, https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx, https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx.*