STATEMENT FOR THE RECORD OF

CANDACE WORLEY, VICE PRESIDENT AND CHIEF TECHNICAL STRATEGIST, MCAFEE, LLC.

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

ON GROWING AND DIVERSIFYING THE CYBER TALENT PIPELINE

MAY 21, 2019, 2:00 PM | 310 CANNON HOUSE OFFICE BUILDING

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 worldwide 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 five and a half years as the Vice President and General Manager of McAfee's Enterprise Endpoint Security business.

MCAFEE'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 three 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, policymakers 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 widespread 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 two 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, policymakers 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 four-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 four-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% of community college students are women and 41% are minorities. Additionally, community college tuition is more economical than a four-year university. In-state community college tuition is about one third the cost of in-state four-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 four-year college students do in the CyberCorps program. Students would receive a two-year certificate in cybersecurity that would be transferrable to a four-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 two, three, or five 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 two to three 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 meantime, 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, standalone 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% of all global hires were female and 13% 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% 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 dialogue
    - 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 Online Safety Program, onsite 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 three awards of $10,000 for the 2019-2020 school year. Twelve students from each of the three 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 firsthand 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 policymakers. 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.