STATEMENT FOR THE RECORD OF

LISA DEPEW, HEAD OF INDUSTRY AND ACADEMIC OUTREACH, MCAFEE

BEFORE THE U.S. HOUSE OF REPRESENTATIVES

INFORMATION TECHNOLOGY SUBCOMMITEE OF THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

ON REVIEWING FEDERAL IT WORKFORCE CHALLENGES AND POSSIBLE SOLUTIONS

April 4, 2017 2:00 PM, 2154 Rayburn House Office Building

Good afternoon, Chairman Hurd, Ranking Member Kelly, and distinguished members of the Subcommittee. Thank you for the opportunity to testify today. I am Lisa Depew, head of industry and academic outreach for McAfee.

I am pleased to address the Committee on federal IT workforce challenges, which we all know is an issue that must be addressed. I will focus on developing cybersecurity professionals, as that is one of the greatest areas of need and also one that we at McAfee know well. My testimony will briefly describe the problem, offer some specific solutions, and conclude by discussing some of the larger issues that are integral to our cybersecurity skills shortage.

First, I would like to provide some background on my experience. For the past two and a half years, I have worked closely with McAfee's Chief Technology Officer, Steve Grobman, to identify, evaluate, and prioritize compelling new technologies and work with technical leaders throughout the company to identify and resolve challenges while building industry-leading security solutions. Currently I drive technical leadership development among our engineering community, focusing on how to maximize growth and impact of McAfee's technical talent. I expand innovation initiatives by driving collaboration with organizations like the Society of Women Engineers and university programs to accelerate partnerships and opportunities between private sector, non-profits, and academia.

Prior to joining the field of cybersecurity, I spent 15 years at Intel Corporation in a wide variety of engineering and business operations roles including microprocessor and memory design, desktop and data center customer enabling, building and managing automation services infrastructure, and streamlining support operations for millions of business PCs worldwide. I have been recognized inside and outside corporations for my advocacy for women in technology and have consulted nationally and internationally on methodologies to attract and retain a diverse and inclusive workforce.

MCAFEE'S COMMITMENT TO CYBERSECURITY

I'm extremely pleased to be able to announce that as of today, McAfee is an independent cybersecurity company which, as a standalone business, is one of the world's largest pure-play cybersecurity firms. We're built on the belief that "Together is Power," and our strategic vision focuses on innovation, trust and collaboration. We recently announced a whole new ecosystem of integrated platforms, automated workflows, and orchestrated systems based on an open

communications fabric that will enable all of us in cybersecurity to work together in ways never before thought possible. So this is a special day for us, and it's a great time to be addressing this important subcommittee.

The Cybersecurity Skills Shortage – By the Numbers

In 2016 Intel Security and the Center for Strategic and International Studies (CSIS) 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.
- The most desirable skills cited in all eight countries surveyed were intrusion detection, secure software development, and attack mitigation.
- 76 percent of respondents say 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 July study, the numbers haven't improved any. The cybersecurity workforce shortage is projected to reach 1.8 million by 2022, according to the most recent Global Information Security Workforce Study. And the number of women in the field has not increased at all, coming in at only 11% globally, according to a Women in Cybersecurity report by the Executive Women's Forum and $(ISC)^2$. In North America, women constitute only 14 percent of the information security workforce. The numbers are even worse for African Americans, who comprise only three percent of information security analysts in the U.S., according to the Bureau of Labor Statistics figures cited in an article in Forbes. Compare these numbers to predicted spending on cybersecurity: Cyber economy research firm Cybersecurity Ventures has predicted that global spending on cybersecurity products and services will surpass $1 trillion cumulatively between 2017 and 2021 and that annual cybercrime costs will reach $6 trillion in 2021. Both figures indicate the serious need for more trained professionals.

The cybersecurity skills shortage is particularly acute in the federal government. Tony Scott, the federal government's former CIO, said in a GovLoop article, "There are an estimated 10,000 openings in the federal government for cyber professionals that we would love to fill, but there's just not the talent available." Given the vital role such government agencies as DoD, DHS and the intelligence agencies play in protecting the United States, this skills gap is disquieting and merits particular attention from policymakers.

One strategy for addressing the cybersecurity skills deficit is to use automation – through machine learning and artificial intelligence. We at McAfee take advantage of this, and our tools incorporate automation in strategic ways. 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 2017 and beyond.

This speaks to the need for investments in IT modernization and modern cybersecurity solutions, which the President's draft executive order addresses. We support these much-needed policy changes. In the meantime, however – and even after legacy IT is retired, replaced and modernized with current generation cybersecurity capabilities – we will still need many more skilled cybersecurity professionals.

RECOMMENDATIONS

What follows are some recommendations for closing the skills gap.

Expand the Current CyberCorps Program

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 is structured as such: The National Science Foundation (NSF) provides grants to about 70 institutions across the country to offer scholarships to 10-12 full-time students each. Students get free tuition for up to two years in addition to annul stipends -- $22,500 for undergraduates and $34,000 for graduate students. They also get allowances for health insurance, textbooks and professional development. Some universities also partner with the Department of Homeland Security (DHS) on these programs.

Students generally must be juniors or seniors and must qualify for the program by attaining a specific GPA, usually at least a 3.0 or higher. Upon completing their coursework and a required internship, students earn a degree, then go 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.

With additional funding, the CyberCorps SFS program certainly could be expanded to more institutions and more students within each of those schools. To date, the federal government has made a solid commitment to supporting the SFS program, having spent $45 million in 2015, $50 million in 2016, and the most recent Administration's budget requested $70 million. As a baseline, an investment of $40 million pays for roughly 1,500+ students to complete the scholarship program.

Given the size and scale of the cyber skills deficit, policymakers should significantly increase the size of the program, possibly something in the range of $180 million. At this level of funding, the program could support roughly 6,400 scholarships. Such a level of investment would make a dent in the federal cyber skills deficit, estimated to be in the range of 10,000 per year. At the same time, this level of investment could help create a new generation of federal cyber professionals that can serve as positive role models for a countless number of middle and high school students across the country to consider the benefits of a cyber career and federal service. Indeed, this positive feedback loop of the SFS program might well be its biggest long-term contribution.

We also recommend that the program include a "give-back" component. The students who enter this program are compensated well, they receive paid internships during their course of study,

and they are in line for federal jobs when they graduate. Yes, they are required to work for the federal government for time equivalent to what they spent in the program, but unlike many other graduates, they have a job in their field where they are enhancing their resumes and skill sets for the future. They also ought to become ambassadors in the community for the program and for solving the cybersecurity talent shortage. They should be asked to participate in a teaching or advocacy role. We would not suggest prescribing the role; rather, the graduates could use their own creativity to propose how they plan to give back. The CyberCorps SFS program should suggest some possibilities, including volunteering in middle and high schools to teach cyber skills on a regular basis, acting as mentors to students, and taking students under their wing during internships the program might establish with the federal government.

Create a Community College Program

While the CyberCorps program serves college juniors and seniors who are already well along the learning path, another program, or an expansion of the SFS program, could seek to attract high school graduates who don't yet have specific career aspirations. Private companies could partner with a community college in their area to establish a course of study focusing on cybersecurity. The federal government could fund all or part of the tuition remission for students. Interested students would be taught both by college faculty and private sector practitioners. For example, an IT company could offer several faculty members/guest lecturers who would participate during a semester. Students would receive free tuition – paid by a federal program, perhaps with private sector contributions – but they would not receive a stipend for living arrangements, as 4-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.

Community colleges tend to attract a variety of students – including recent high school graduates but also returning veterans and other adult students who might have pursued other careers or might even be working full- or part-time. The community college option could also further ethnic and racial diversity in a cyber program – something that is badly needed. This diversity would be a plus rather than a minus for the cybersecurity profession, as the field requires a diverse set of skills and individuals. Not all of these skills are strictly technical, and for those that are technical, not all require high levels of formal education. You don't need a Ph.D. – or even a bachelor's degree – to work in cybersecurity. For instance, a four-year degree is not necessarily required to work in a security operations center (SOC). 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.

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

We Need Cultural Changes to Close the Cyber Skills Gap

Cybersecurity is one of the greatest technical challenges of our time. We need more people – in addition to continually advancing technology, of course – to address this challenge. So far, we've addressed specific programs that can train individuals who have reached at least 18 years of age and might have some interest in pursuing a cybersecurity career. Now I want to step back and take a wider look at the challenges we as a society face in developing those people. I want to focus on three in specific:

- Empowering more children to understand and embrace STEM, security and privacy
- Changing the image of a cybersecurity professional, and finally,
- Addressing the gender and diversity gaps

We Need More Awareness of STEM, Security and Privacy

We've heard it before, we'll hear it again, but it still deserves an important mention: We need to invest more in exposing grade school and middle school students to science, technology, engineering and math (STEM). "The future of the economy is in STEM," says James Brown, executive director of the STEM Education Coalition in Washington, D.C., adding the most recent Bureau of Labor Statistics finding that employment in STEM jobs is projected to grow to more than nine million between 2012 and 2022. That sounds like a conservative estimate to me, and indeed it probably is. While various initiatives have sprung up to address the STEM education problem, we're not there yet – and we need to be. We need a broad-based STEM investment plan to solve this long-term problem.

But it's not just STEM awareness that children need at an early age. It's also awareness of security and privacy. As adults we hear about breaches in the news, and some of us understand cyber is a corporate board room topic, but does the average grade school and middle school student learn about the importance of cyber safety? Do they understand what that means beyond "don't share your password"? Where does security sit on the average college student's list of priorities? Look at topics affecting America's youth today: the shifting economy, cyberbullying, high rates of human trafficking (most which is executed via social media and digital transactions). We have a great opportunity to increase awareness about security as at affects the workforce at large (1.5 million unfilled jobs today and growing, steady pay, high job security) but also in a way that appeals to our millennial generation – a group passionate about causes, especially human interest ones— and generation X youth, who are learning about how to keep themselves and their friends safe. We need both traditional and creative approaches to reach these students, possibly through gamification.

We also need to systemically change the conversation around cybersecurity and raise awareness with young children in the community. America needs to instill stronger cyber safety awareness. How many times do we wash our hands a day, because we know it's key to staying healthy? How many kids put on their seatbelts without thinking, because it's a routine behavior to stay safe? We need to get to that same level of unconscious competence and cybersecurity precaution with our digital lives, and education must start with our youth. Then, once our children are attuned to cyber safety being a part of their daily lives, making the jump to choosing a career as creator/leader/protector in cyber becomes a simpler sell.

We Need to Rebrand Cyber

What does the average person envision when they think "cybersecurity"? We have to move beyond the stereotype of "hacker in a hoodie." This persona commonly elicits images of male, devious, and loner. Yet security is increasingly about creative, collaborative, and together. High-impact, valuable cybersecurity professionals can—and do—come from all walks of life, with broad and varied backgrounds. It is their diverse skills and experience that enable them to identify the corner case, look at the technology in a way other than it was intended, and think outside the box to determine how an attacker might exploit a system. The legacy tech innovator Bell Labs proved that diverse teams produce more creative, high-quality products. Similarly, a diverse incident response team will look at solutions from a multitude of perspectives and be more holistic and resilient in addressing the breadth of tomorrow's cybersecurity challenges. The attacker only has to be right once; the defense has to be accurate 100% of the time. A more diverse set of capabilities, mindsets and domains of expertise will enable the creative, broad, holistic thinking that will continue to be crucial to America's national defense.

We need to reframe how we "sell" cyber, and that starts with talking in a way that will resonate with America's youth. When you ask a 10-year old, "Who wants to be a cybersecurity professional?", I dare say you'll get a lot of blank stares. But when you say, "Who wants a job where they get to be creative and help people? Who likes to work on teams and solve puzzles?" you get a much larger pool of raised hands—girls' and boys'.

We also need to increase our focus on diversity. Diversity isn't about checking a box to meet a gender or ethnicity requirement. It's about building a robust team with a rich blend of capabilities and perspectives. I'll use a sporting analogy, as a tribute to my Cubs fan husband and our sports enthusiast CEO, Chris Young. Building a diverse organization is like drafting a baseball team. You need highly talented individuals, without question. But fielding a team of nine exceptional pitchers is not the recipe for success. The strength of high-performing teams is in having a variety of experts, each world-class in his or her domain. It's the collaboration and execution across the domains that empowers the team to win. This also means focusing on diversity of race, ethnicity, gender and age – all of which can expand a team's perspective and ultimately serve customers more creatively and effectively.

Cyber-attacks are certainly diverse and complex; worldwide incidents range in scope from organized crime to recreational vandalism to hacktivism to state sponsored cyberattacks. We cannot understate the importance of diversity and partnerships in orchestrating effective cybersecurity defense. It's about having the breadth and the depth of backgrounds, skills, and experiences that enable a team—and the worldwide cyber community—to respond to and mitigate innumerable threats, many of which haven't even been invented yet. "Together is Power" is not just a tagline. It's a fundamental requirement to cybersecurity practitioners being successful in our mission.

The great company I recently worked for, Intel, has long had a commitment to diversity, believing that "creating an inclusive environment [enables] all Intel employees [to] be full empowered to take on the world's most complex and challenging problems," according to Danielle Brown, Intel chief diversity and inclusion officer. In the new McAfee, we plan to sustain a commitment to diversity and inclusion. It's not only the right thing to do; it's the smart thing to do.

We Need to Close the Gender Gap

The cybersecurity profession stands to profit greatly from diversity across many sectors. As a woman in cyber, I want to zero in briefly on closing the cyber gender gap. To again cite the Women in Cybersecurity report, only 14 percent of cybersecurity professionals in the U.S. are women. Clearly, training and recruiting more women could help alleviate the skills gap. Let me suggest some ways we can help do that. Interestingly, many of what society traditionally considers "feminine" traits are highly valuable in cyber—collaboration, teamwork, creativity, and consensus-building, to name a few.

We need to make the cyber landscape a place where these skills are lauded, not minimized. If we want to appeal to broader audiences, we must be inclusive of broader skills and experiences. While hackathons holding timed competitions for those who can pick the most locks may appeal to the competitively driven traditional hacker, we should augment these offerings with additional engagements focused on collaboration, teamwork and solution-building. We can focus on skills needed for success--using neutral or positive terminologies. For example, we can swap "devious" for "clever"; nurture passions for creativity and puzzle-solving; turn "what can I break?" into "what can I help fix?"

Additionally, we can both appeal to more women and woo more philanthropy-minded individuals by better explaining how our work helps people. If you look at the stats for women engineering graduates, the numbers are highest in biomedical engineering and environmental engineering—fields where students can draw a direct correlation to helping humanity. Cyber is clearly a field that helps protect and empower people. If we brand the domain effectively, we have a target-rich environment of highly capable girls and women who could be joining the ranks to fill that 1.5M-person deficit.

We Can Address Multiple Challenges Simultaneously

Rather than starting from scratch, we have significant opportunities to build on existing infrastructure. Extensive work has been done already to inspire youth to become interested in coding—how do we augment that to include a focus on cyber? *Girls Who Code* has an extensive national base and is graduating its first collegiate classes. What can be done to encourage focus on secure coding in their curriculum? Do GWC and similar programs talk about job possibilities in cybersecurity? The Society of Women Engineers has a national membership of thousands; are we leveraging that community for skills retraining, seeking experts in adjacent fields, and providing role models for women in technology? What is being done for inner city multi-racial and multi-cultural youth? Foster youth are at risk of becoming "lost in the system" and are an extremely high at-risk group to be victims of human trafficking. Can we target this population for a skills-development pilot, offering them the opportunity for a cyber education while helping combat a larger societal problem?

The afore-mentioned study Hacking the Skills Shortage also includes recommendations for closing the cybersecurity skills gap through increased diversity and creative approaches to training. The authors write, "Our research suggests that cybersecurity education should start at

an early age, target a more diverse range of students, and provide hands-on experiences and training."

In my experience, people are far more passionate and committed to a cause they have personal experience with. Look at the athlete with a sporting injury who became a physical therapist or the child whose parent was killed who became a police officer. How do we leverage personal circumstances to entice and inspire youth toward a career that helps humanity through cybersecurity? We have to start thinking outside the box, and I suggest one way is to get more personal. That way we can both find and support people who will be in the career for the long haul.

Recruiting and Skills Identification

Regarding standing up a cybersecurity talent development program, it's easy to ask, "What degrees do I need?" or "What certifications should I require?" As a process-minded engineer, I fully understand the desire to have a formulaic approach to addressing this talent shortage problem. Discussions will be had. Processes will be built. I urge us to keep top of mind the long-term objective. 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. As a hiring manager and technical talent developer, though, 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.

Prioritizing Time for Advocacy

Lastly, I would like to stress the importance of allocating time for advocacy by current cyber professionals to enroll and enlist the next generation. As a woman in tech (who spent several years working part-time as a new mother), 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 is extremely difficult to deliver excellence in your day job and carve 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 such a distinguished panel of policymakers. Both Chairman Hurd and Ranking Member Kelly merit praise for their dedication to closing the cybersecurity skills gap. This gap can be closed, but it will take a true public-private partnership to do so. Toward that end, we need to increase the funding level of the CyberCorps Scholarship for

Service program. The IT sector needs to collaborate closely with the government to ensure that students and recent graduates of this program are given many opportunities to take part in co-ops and internships that support the acquisition of cybersecurity skill sets. We also need to broaden our point of view of what it means to be a cybersecurity professional. The days of thinking about cyber experts in a one-dimensional manner – the guy with the hoodie – are over. The future is about ensuring that the widest diversity of people and skill sets are brought into the cybersecurity profession so we can meet the challenges of protecting public and private sector institutions from an array of cybersecurity threats.

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