STATEMENT FOR THE RECORD OF

SCOTT MONTGOMERY, VICE PRESIDENT & CHIEF TECHNICAL STRATEGIST, MCAFEE, LLC.

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

ON THE CHALLENGES OF RECRUITING AND RETAINING A CYBERSECURITY WORKFORCE

September 7, 2017, 2:00 PM | HOUSE CAPITOL VISITOR CENTER (CVC) ROOM 210

Good afternoon, Chairman Ratcliffe, Ranking Member Richmond, and members of the Subcommittee. Thank you for the opportunity to testify today. I am Scott Montgomery, Vice President and Chief Technical Strategist of McAfee, LLC.

I am pleased to address the subcommittee on the challenges of recruiting and retaining a cybersecurity workforce. My testimony will address the broad contours of the cybersecurity skills shortage, both in the public and private sectors, and what we can do about it. One involves people: training more, broadening our perception of what attributes and skills are needed, and incentivizing government investments in cyber specialists. The other involves technology: moving to the cloud, using automation wisely, and encouraging industry to move to interoperable platforms.

First, I would like to provide some background on my experience and McAfee's commitment to cybersecurity. I help drive the company's technical innovation, evangelize our expertise, thought leadership, and offerings to public and individual audiences; and work to increase the public trust by cooperating with law enforcement on cybercriminal investigations and disruption. With more than 20 years in content and network security, I bring a practitioner's perspective to the art and science of cybersecurity. I have designed, built, tested, and certified information security and privacy solutions for such companies as McAfee, Secure Computing, and on behalf of a wide variety of public sector organizations.

MCAFEE'S COMMITMENT TO CYBERSECURITY

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other industry products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, we secure their digital lifestyle at home and away. By working with other security players, we are leading the effort to unite against state-sponsored actors, cybercriminals, hacktivists, and other disruptors for the benefit of all.

THE CYBERSECURITY SKILLS 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.
- 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. According to a recent Global Information Security Workforce Study, the cybersecurity workforce shortage is projected to reach 1.8 million by 2022. The cybersecurity skills shortage is equally troublesome 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 the Departments of Defense and Homeland Security as well as the intelligence agencies play in protecting the United States, this skills gap is disquieting and merits attention from policymakers.

None of this is news. We've studied this workforce shortage for several years now, and if we're serious about its importance we need to do something about it immediately. Following are some recommendations for training and incentivizing more people and also using technology to help fill the gap.

TRAIN AND CROSS-TRAIN MORE PEOPLE

Expand the Current CyberCorps Program

First, we need to focus on expanding existing programs that train people in the cybersecurity field. For example, 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 so that The National Science Foundation (NSF) provides grants to about 70 institutions across the country to offer scholarships to 10-12 full-time students each. With this structure, 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.

Generally, students 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 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 requesting $70 million. As a baseline, an investment of $40 million pays for roughly 1,500+ students to complete the scholarship program.

With the cyber skills deficit being substantial, policymakers should significantly increase the size of the program, possibly something in the range of $180 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. 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 a countless number of 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.

Create a Community College Program

While the CyberCorps program serves college juniors and seniors who are already well along the learning path, we believe 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). As pointed out earlier, a strong security operation requires various 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.

Encourage Cultural Changes to Close the Cyber Skills Gap

As cybersecurity is one of the greatest technical challenges of our time, we need to be creative in attracting more people to the workforce. One of the ways we can do this is by changing our way of thinking about the industry. Cybersecurity professionals can—and do—have broad and varied backgrounds. Diverse skills and experience can enable them to examine problems from a different perspective, bringing creativity rather than just linear thinking to cyber problems and solutions. The legacy tech innovator Bell Labs proved that diverse teams produce more creative, high-quality products. Likewise, a diverse incident response team can benefit from look at cyber incidents and responses from a multitude of perspectives.

We must also address the gender and diversity gap, which would help alleviate the skills gap. In North America, women constitute only 14 percent of the information security workforce, according to a Women in Cybersecurity report by the Executive Women's Forum and (ISC). 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. Research on large, innovative organizations has shown that gender and racial diversity improves the 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.

Pass Legislation like the "Cyber Scholarship Opportunities Act of 2017"

I'd also like to take a moment to applaud the recently approved "Cyber Scholarship Opportunities Act of 2017" that was passed through the Senate Commerce, Science and Transportation Committee, as well as Chairman McCaul's "Cyber Scholarship Opportunities Act of 2017." Both bills require the SFS program to include students pursuing an associate's degree in a cybersecurity field without the intent of transferring to a bachelor's degree program, people who have a bachelor's degree already, or people who are veterans of the Armed Forces.

This is encouraging news for closing the skills gap at the operator and junior analyst levels. McAfee supports these bills and hopes they get signed into law. However, there is still more work to be done. The Senate bill directs the NSF to provide awards to improve cybersecurity

education and increase teacher recruitment. We hope the Senate considers those with hands-on cybersecurity experience as potential candidates for teaching.

The Thorny Problem of the Government's Gap

The cybersecurity skills gap also extends to government. Quite simply, the public sector can't keep up with the private sector in terms of pay scale and benefits. We have to change that to be able to attract and retain excellent cyber professionals in the public sector. To date, the SFS program has been particularly effective in adding to cybersecurity talent in the government. While all graduates are required to begin their careers by serving in the government, an impressive 70%, according to NSF, actually remain in government jobs. I'd like to unpack this issue a bit and distinguish between different types of cyber professionals in government organizations.

At a very high level, there are three categories of cyber professionals. First there are operators – the people who implement the security technology and keep it running in systems and networks. You don't need a Ph.D. in computer science to fill an operator role, and in fact the government has a good supply of such people either directly or through contractors. Then there are researchers, people who explore the latest in cyber defense. Again, the federal government is well-served here by labs in the Department of Defense, DARPA, IARPA and the intelligence community. The third category is analysts – the people who can respond to a breach in the first few minutes and conduct the necessary analytical work to understand the implications of an attack and develop a remediation plan. This is the area where the government has the most serious need and where they need people who are not just technically trained but also astute and creative problem-solvers.

In order to attract this kind of talent, the federal government needs to find ways to incentivize people and reduce obstacles to them serving in cybersecurity positions. The salary issue cannot be overlooked, as this is a major incentive for most professionals – especially in the most sought-after areas of IT like cybersecurity. Government needs to offer competitive salaries, and if that's not possible, government should offer better retirement packages to be more on a par with the private sector. Alternatively, agencies could offer cybersecurity personnel the ability to up-level their positions (e.g., from a GS12 to a GS13) more quickly than usual.

Congress gave DHS expedited hiring authority for cybersecurity three years ago – an authority that could address many of these suggestions. It's incumbent upon the Department to move these plans forward as soon as possible.

Another impediment to getting cybersecurity personnel where they need to be in government agencies has to do with clearances. Often an agency will require an advanced clearance to enter a facility when, in fact, many of the systems don't house classified data. As there's a limited number of personnel with high-level security clearances – and as it takes a long while to get one – this also contributes to the cybersecurity talent shortage in government. Expediting the

vetting process and carefully reviewing which clearances are truly necessary to work on a system, while still protecting national security, would both be steps in the right direction.

Another topic that deserves attention is the need to review and declassify materials over time. This merits a lot more study, and I know there are efforts within the Defense Department, in particular, to better determine what data actually needs to be classified and for how long. If data were to be declassified more quickly, more cybersecurity professionals with lower or no clearances would be able to be of service.

Public-Private Sector Cross Pollination

We must also develop creative approaches to enabling the public and private sectors to share talent, particularly during significant cybersecurity events. Cybersecurity is a rapidly changing area, and what's valid today might well be superseded tomorrow. 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 cyber security 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 hack 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 cyber security 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 technology more and more.

Moving to the Cloud

Both the government and industry are moving their IT operations to the cloud. Last year, McAfee surveyed over 2,000 professionals for our annual cloud security research study, Building Trust in a Cloudy Sky: The State of Cloud Adoption and Security. We found that hybrid cloud

adoption tripled in the last year, increasing from 19% to 57% in organizations surveyed. Additionally, IT executives believed their IT budget would be 80% cloud-based within an average of 13 months, and 73% of companies are planning to move to a fully software-defined data center within two years.

Here's the relevance to the workforce shortage: As more organizations move to the cloud, the cloud providers rather than the organizations are delivering a baseline of foundational technology – hardware, operating systems, and so forth. This reduces the overall amount of labor that an organization's IT and information security staff needs to exert, leveraging cloud's inherent economies of scale. However, the move to the cloud will not, by itself, close the cyber skills gap in the short run; there are just too many open slots to fill. Indeed, our recent cloud study also found that 49% of businesses are currently delaying cloud deployment due to a cybersecurity skills gap. Nevertheless, the move to the cloud will help reduce the labor shortage; it will just take more time to pay off as more organizations offload their IT environments to cloud providers.

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 2017 and beyond.

This speaks to the need for investments in IT modernization and modern cybersecurity solutions, which the President's executive order addresses. 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 (the cybersecurity analysts referred to earlier). 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.

Fostering Interoperability

When considering the role of security technologies, it's important to understand the market-like forces that drive the effectiveness of cybersecurity defense. Most information technologies continuously improve over time. Paradoxically, cyber defense technologies do not follow this pattern. Their effectiveness peaks shortly after release and then degrades. When a new defensive capability is first released, bad actors take little notice, but once deployed at scale, they adopt evasion tactics and counter-measures, causing the effectiveness to significantly degrade.

Where does that leave us? We see the current paradigm of constant integration of point products – individual software applications – as ineffective and unsustainable, particularly given the substantial number of cyber professionals needed to knit together disparate systems. Not only are technology efficiencies already declining by the time the lengthy purchase and integration cycles are complete, but organizations are unable to deal with the complexity of supporting upwards of 30 or 40 independent tools and technologies. That's a losing game, but it's the one security practitioners find themselves playing.

We need a different approach where technology – enabled with strong collaboration -- can be deployed rapidly to security platforms so they can communicate with each other over open communication protocols. Organizations in both the public and private sector need security tools that are interoperable and interchangeable to protect against existing and prospective threats. As cybersecurity solutions become interoperable, they become more efficient and cost-effective. They also become easier to maintain than a IT environment of disparate systems, the classic IT hair ball. Over time, more interoperable cybersecurity systems will contribute to closing the skills gap as they get more widely deployed. We call on the cybersecurity industry to design technology to an open standard, on an open platform, so customers are not locked into proprietary technologies that don't work with each other or allow for change.

McAfee has taken a major step toward fostering interoperability by opening our Data Exchange Layer (DXL) – a communications fabric that enables unprecedented collaboration in an open-source, real-time system – to other developers and vendors to use at no expense. OpenDXL™ is at the core of our mission to enable security devices to share intelligence and orchestrate security operations at rapid speed. As of today, there are 13 companies connected to the DXL ecosystem, 12 others in testing or development, and 14 additional companies in the design phase.

OpenDXL is a big part of what we mean by Together Is Power. No single industry partner can cover the vast spectrum of security and privacy problems. No single industry partner will catch every issue every time. Only by working collaboratively in the private and public sectors can we defeat cyber attackers. This means bringing the best ideas, the best technologies and the best people to bear on our common security problem. It means leveraging technologies guided by the strategic intellect that only humans can provide. And to ensure that we have enough

human intellect to work with our continually evolving technology, we need to encourage more people from diverse backgrounds to enter the cybersecurity field, train them, and – particularly in the case of government – reward them.

I look forward to our discussion and will be happy to answer any questions.