WRITTEN STATEMENT FOR THE RECORD OF SCOTT MONTGOMERY, VICE PRESIDENT, INTEL SECURITY GROUP CHIEF TECHNICAL STRATEGIST, before the UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON INFORMATION TECHNOLOGY, "Hearing On Closing the Talent Gap in Federal IT"

SEPTEMBER 22, 2016

Good afternoon Chairman Hurd, Ranking Member Kelly, and members of the committee. Thank you for the opportunity to testify today. I am Scott Montgomery, Vice President and Chief Technical Strategist, Intel Security Group, part of Intel Corporation. I am pleased to address the committee on the challenges facing the federal government and the private sector in hiring and retaining qualified cybersecurity professionals. The shortage of these professionals is an interconnected challenge, one that impacts both public and private sector organizations given the common threats they face and the mobility and increasingly connected nature of today's work force. As a member of one of the world's leading cybersecurity companies, my testimony will focus on the skills gap in the cybersecurity ecosystem of companies and governments, and what the government, in collaboration with the private sector, can do to close it.

First, I would like to provide some background on my experience and Intel's commitment to cybersecurity. I work for the Intel Security Group Chief Technology Officer (CTO) and manage the worldwide team that carries CTO titles. Together we 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 a wide variety of public sector organizations.

INTEL'S COMMITMENT TO CYBERSECURITY

Intel is a global leader in computing innovation, designing and building the essential foundational technologies that support the world's computing devices. Combining Intel's decades-long computing design and manufacturing experience with Intel Security's market-leading cybersecurity solutions, we bring a unique understanding of the cybersecurity challenges threatening our nation's digital infrastructure and global e-commerce. Governments, businesses, and consumers face a cybersecurity threat landscape that is constantly evolving every day with each new technology that is brought to market at a faster pace than ever before. The sharp rise of internet-enabled devices in government, industry, and the home exacerbates this already difficult challenge. It is thus critical that we collaborate and coordinate our efforts across the public and private sectors to ensure the safety and prosperity of our collective digital future while promoting innovation, protecting citizens' privacy and civil liberties, and preserving the promise of the Internet as a driver of global economic development and social interaction.

With the rising volume and complexity of threats, the shrinking time and resources available to handle them, and now the dramatic increase in internet-enabled devices and delivery mechanisms such as cloud computing, security practitioners must evolve their approach. The job hasn't changed: protect vital services and data from theft, manipulation, and loss due to external and internal adversaries. But we need to change the way we do the job by focusing on ways to reduce security fragmentation, automate tasks, and force-multiply capabilities.

Intel Security believes that a platform-driven approach best enables organizations to effectively block threats, identify compromises, and expedite remediation. It's at the center of our commitment to making what we call the "Protect, Detect, and Correct" life cycle easy for organizations to deploy to enable a safe and connected world. Focusing on open, integrated solutions to work within a platform and placing a premium on the development of easy-to-use customer interfaces can expedite the threat defense life cycle and help organizations optimize the use of valuable resources like trained cybersecurity professionals.

THE THREAT LANDSCAPE

Over the past decade, attackers have evolved from recreational "hackers" with limited capabilities to organized crime and state-sponsored adversaries with dedicated resources and highly skilled personnel. At the same time, as organizations become increasingly reliant on digital infrastructure, security breaches can have a more pervasive and cascading impact on data security and operational resiliency. Organizations are more vulnerable in more places.

Adversaries are now capable of commandeering strategic assets and critical infrastructure. Yet most organizations still lack the resources necessary to adequately monitor their networks and defend against increasingly sophisticated attacks.

Add to that the sobering realization that while adversaries' goals remain relatively easy, trying to find the lowest hanging fruit in terms of a weak system or an undertrained or cooperative insider, defenders must be impenetrable 100% of the time. Today we realize as an industry this goal is mathematically unlikely to be achieved, even for properly funded and adequately staffed security vendors or large corporations.

The Global Cybersecurity Skills Gap:

Earlier this year, the Center for Strategic and International Studies (CSIS), in partnership with Intel Security, released "Hacking the Skills Shortage", a global report outlining the talent shortage crisis impacting the cybersecurity ecosystem across companies and nations. The results of the research were both stunning and informative.

A majority of respondents (82 percent) admit to a shortage of cybersecurity skills, with 71 percent of respondents citing this shortage as having a direct and measurable impact on organizations whose lack of cyber talent makes them more attractive hacking targets.[1] In 2015, 209,000 cybersecurity jobs went unfilled in the United States alone.[2] Despite 1 in 4 respondents confirming their organizations have lost proprietary data as a result of their cybersecurity skills gap, there are no signs that this workforce shortage will abate in the near-term. [3] Respondents estimated an average of 15 percent of their company's available cybersecurity positions could go unfilled by 2020.[4]

If the demand for cybersecurity professionals continues to outpace the supply of qualified workers—and all the evidence suggests it will—the United States could

[1] Center for Strategic and International Studies, *Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills*, p. 4, (May 2, 2016), http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

[2] Id. at 5.

[3] Id. at 7, 8.

[4] Id. at 7.

face a cybersecurity skills deficit of around 1 million workers in the next 5 to 10 years.[5] With the increase in cloud, mobile computing, and the Internet of Things, as well as advanced targeted cyberattacks and cyberterrorism across the globe, the need for a technically stronger and numerically increased cybersecurity workforce is critical.

Intel's Commitment to Closing the Skills Gap:

Public Private Partnerships

Given the current cybersecurity skills shortage, organizations across the spectrum cannot manage their protective defenses alone. Security is a shared goal carrying a shared responsibility. As a result, the strategic partnerships that have grown between public and private sector entities over the last two decades have never been more important.

At a national level, critical industry sectors supporting the safety, security, and economic growth of the United States were among the first to self-organize in partnership with government agencies to assess and mitigate threats to U.S. critical infrastructure. These public-private partnerships are fueled by a joint commitment to defend critical infrastructures against increasingly sophisticated cyberattacks, and they thrive on sharing threat indicators, best practices, and incident response in a mutual, non-regulatory environment.

Intel has been active in many of these partnership initiatives for more than 10 years. Just a few important examples where Intel has a leadership presence include:

- President's National Security Telecommunications Advisory Committee
- Information Technology Sector Coordinating Council
- Information Technology Information Sharing and Analysis Center
- National Cyber Security Alliance
- National Cybersecurity Center of Excellence
- Cybersecurity Framework

Through these partnerships, Intel works to provide hardware, software, and training to advance the rapid adoption of secure technologies around the country. In addition, we remain actively engaged in the development of new cybersecurity

[5] Id. at 5.

guidelines to help public and private sector organizations evaluate their security postures and conduct risk assessments, regardless of size or sophistication.

As these partnerships grow and mature, our company will continue to invest, engage, and contribute. The challenge is never-ending, but we have no doubt that the public-private partnership model will continue to protect and serve our national interests well into the future.

Intel's Investment in Education

Intel believes that young people are the key to solving these global challenges. A solid math and science foundation coupled with such skills as critical thinking, collaboration, and problem solving are crucial for their overall success and the competitiveness of the United States. By making significant investments in STEM programs at high schools and universities, we are addressing one of the most pressing elements of our nation's technology skills deficit and giving students the core skills they need to join the cybersecurity work force. For instance:

- Intel has invested over $1 billion and Intel employees have donated over 5 million hours in the past decade toward improving STEM education in the U.S. and internationally.

- We have invested over $670 million in university programs since 2001 to foster the next generation of technology innovators and leaders. We are collaborating with 700 researchers and 95 universities to enhance teaching resources, develop student courseware, and fund world-class research and technology competitions in information technology fields like security, cloud, and big data.

- Our internship program funds over 100 paid internships each year, providing undergraduate and graduate students with opportunities to work on complex projects that span our product portfolio, including security.

- We have invested more than $100 million annually in programs that promote STEM education, encourage women and girls to seek careers in technology, foster and celebrate innovation and entrepreneurship among the best and brightest young students in the world, and help teachers incorporate best practices in math, science, and classroom technology in their work.

- Our cybersecurity business unit takes pride in empowering families with the tools they need to defend themselves from online threats ranging from cybercriminals to cyberbullies. In 2009, Intel employees began volunteering to teach school-aged children how to use their digital devices responsibly in pilot programs across the United States. Since the original launch of McAfee Online Safety for Kids, the program has vastly grown and maintains a wide global reach. To date, Intel volunteers have educated more than 250,000 children, parents, and teachers worldwide about how to remain safe and secure online.

- Our cybersecurity business unit also donates coursework and professional services through partnerships with a number of flagship state universities, including Purdue and UMass Amherst, to enable students to successfully train in the cybersecurity operations centers that protect their institutions and come away with valuable work experience.

Policy Recommendations to Close the Skills Gap:

In addition to many other sound policy recommendations, the President’s Cybersecurity National Action Plan (CNAP) takes steps to reverse the cyber talent shortage in the United States with a $62 million increase in spending to expand cybersecurity training and education programs. In particular, the Plan would build out the existing CyberCorps Scholarship-for-Service (SFS) program, providing cyber education scholarships to Americans seeking to serve their country in the federal civilian government. This investment represents a great step forward, but we must be prepared to do much, much more.

The fierce competition over qualified cybersecurity practitioners that currently exists between the public and private sector will continue unless we can begin producing enough new recruits each year to fill the skills gap. That is why we recommend an even larger financial investment in existing federal cyber workforce and education programs, a diversity of career paths for interested students, and stronger coordination on education and workforce initiatives with the private sector.

As Intel Security Senior Vice President and General Manager Chris Young and Chairman Hurd have urged in the past, the government should consider the creation of a Cyber National Guard program. The CyberCorps Scholarship-for-Service and Reserve programs are ideally situated for students looking to pay back their scholarships up-front, with two or three years in federal service. But for students interested in serving their government while jumpstarting a career in the private sector, creating an alternative path to scholarship repayment could bring even more talent to bear. At the state or federal level, an expanded SFS or SFS-style grant program could train and educate a new class of cyber practitioners prepared to serve their government on a full-time, part-time, or as-needed basis while gaining critical experience with cutting-edge private sector innovations. The National Guard has had great success producing talented individuals with diverse skill sets, ready to serve their country in times of need, and it would be worth considering how to apply a similar formula to a cybersecurity context.

The private sector must also be prepared to level-up its partnerships with the government and others in industry to ensure a steady supply of worthwhile internships, co-ops, and training opportunities. In the CSIS report, a lack of quality training opportunities was cited as a significant reason why cyber practitioners seek alternative employment.[6] For this reason, it is not only imperative that public sector entities compensate their cyber professionals well, but also provide ample opportunities for employees to learn new skills and train on new technologies. With more robust public-private partnerships in this area, private companies in different industries can reach individuals at every stage in their career and engage them with new opportunities to learn about a wide variety of digital environments and next-generation technologies.

Finally, investing in technologies capable of reducing the burden on existing human resources and modernizing outdated IT systems will benefit organizations of all sizes. The CNAP invests over $19 billion in cybersecurity as part of the President’s Fiscal Year (FY) 2017 Budget. This represents more than a 35 percent increase in cybersecurity spending from the FY 2016 budget, a necessary investment to help secure our nation in the future. The Plan also calls for a $3.1 billion Information Technology Modernization Fund to modernize government IT systems and transform cybersecurity management. This initiative would enable the retirement, replacement, and modernization of legacy IT that is difficult to secure and expensive to maintain. Just last week, the House Committee on Oversight and Government Reform Committee reported the Modernizing

[6] *Hacking the Skills Shortage* at 19.

Government Technology Act of 2016 out of committee that authorizes the Administration's Information Technology Modernization Fund. By ensuring that these programs invest in truly cutting-edge information technology solutions that benefit from increased automation, user-friendly interfaces, and strong cybersecurity capabilities, Congress can make a vital contribution to securing critical federal assets.

These education and workforce investments, in tandem with CNAP's other cyber initiatives, will make a vital down payment to help close cybersecurity skills gaps in government and the private sector. Intel is committed to supporting the CNAP's cyber workforce efforts and expanding initiatives like the CyberCorps SFS program, but only the federal government can lead the response. The CNAP is a great step forward, but to remedy our alarming cyber talent deficit we will likely need to recruit more than a million Americans trained in cybersecurity and information assurance.

Conclusion:

I would like to once again thank this distinguished panel for giving me the opportunity to discuss the challenges facing the federal government and the private sector in hiring and retaining qualified cybersecurity professionals. We believe that public-private collaboration will continue to be an effective defense against cyberattacks growing in frequency and sophistication. While much progress has been made, more needs to be done—particularly to close the cyber skills gap nationwide. The government should expand the CyberCorps Scholarship-for-Service and Reserve programs and consider creating a Cyber National Guard program to give students new options to pay back their cybersecurity scholarships with federal service. The government should also increase investments in modern, secure information technologies to help protect federal agencies and enable CIO's to effectively leverage their scarce pool of cybersecurity talent. Paying down these "cyber debts" in people and technology will require both industry and government to step up and make hard choices, and Intel looks forward to continuing our engagement on these matters in the future.

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name: Scott Montgomery

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

None

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

Intel Corporation. Vice President and Intel Security Group Chief Technical Strategist.

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

None pursuant to House Rule XI, Clause 2(g)(5)(B) & (C).

I certify that the above information is true and correct.

Signature: DocuSigned by: Scott Montgomery 0296BA8154424C3...

Date: 9/20/2016

Scott A. Montgomery

Scott A. Montgomery is vice president and chief technical strategist for the Intel Security Group at Intel Corporation. He manages the worldwide team of chief technology officers who lead the group's various business units and is responsible for advancing technical innovation in Intel's security solutions.

Montgomery has dedicated his career to information security and privacy software development, gaining a breadth of expertise that spans endpoint protection, firewalls, intrusion prevention, encryption, vulnerability scanners, network visibility tools, mail and Web gateways, authentication, and embedded systems. He joined the Intel organization in 2011 with the acquisition of McAfee Inc., now a wholly owned subsidiary that operates as the Intel Security Group.

Before assuming his current position in 2015, Montgomery was chief technology officer for McAfee's public sector and Americas business units. He oversaw worldwide government certification efforts and worked with industry leaders, government leaders and public sector customers to help ensure that technologies, standards and implementations addressed data security and privacy challenges. His efforts helped drive government and cybersecurity requirements into McAfee products and services and guided the company's policy strategy for the public sector, critical infrastructure and threat intelligence.

Earlier in his career, Montgomery spent six years at Secure Computing Corporation (acquired by McAfee in 2008), where he was responsible for worldwide product management and corporate strategy. He attended Syracuse University.