WRITTEN STATEMENT FOR THE RECORD OF PATTY HATTER, VICE PRESIDENT AND GENERAL MANAGER, INTEL SECURITY PROFESSIONAL SERVICES ORGANIZATION, INTEL CORPORATION

Before the UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON INFORMATION TECHNOLOGY, Hearing On "Cyber Threats, Priority Issues for Cybersecurity Strategy and Expectations for the Cybersecurity National Action Plan (CNAP)"

JUNE 20, 2016

Good morning Chairman Hurd, Ranking Member Kelly, and members of the committee. Thank you for the opportunity to testify today. I am Patty Hatter, Vice President and General Manager of the Intel Security Professional Services Organization, part of Intel Corporation. I am pleased to address the committee on the importance of the Cybersecurity National Action Plan and of understanding and addressing the current and emerging cyber threats facing our nation. I am particularly excited to be speaking here in the great city of Chicago. Intel has a robust footprint in Illinois, with around 100 employees focused on software development in Champaign and another 90 employees based here in Chicago engaged in sales and marketing activities.

My testimony will focus on Intel's commitment to cybersecurity and how we approach an increasingly interconnected threat landscape, as well as the aspects of the CNAP that we hope will strengthen existing public-private partnerships and enhance our national cybersecurity posture in an increasingly digital world.

First, I would like to provide some background on my experience and Intel's commitment to cybersecurity. I have more than 25 years of experience leading operations and technology organizations at several Fortune 500 companies, and currently serve on multiple advisory boards including for the Silicon Valley Education Foundation. I joined Intel Corporation in 2011 with the acquisition of McAfee Inc., which has now been fully integrated into Intel Corporation as part of the Intel Security Group business. As CIO and Vice President of operations at McAfee, I oversaw a global transformation of IT and operations, turning the team into an asset that supported broader enterprise-wide cost savings and revenue growth initiatives across McAfee.

Before joining McAfee in 2010, I was vice president of business operations at Cisco Systems, Inc., where I was responsible for increasing growth, scalability, and revenue by improving integration between Cisco's systems and processes. I began my career at AT&T Inc., where I spent 15 years in various leadership positions in the United States and Europe. I earned my bachelor's and master's degrees in mechanical engineering from Carnegie Mellon University.

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. Recognizing the global trends toward interconnectivity and reliance on digital infrastructure, Intel has also prioritized security across our entire solution set. Indeed, we view cybersecurity as one of the three

computing pillars around which we concentrate our innovation efforts, along with power-efficient performance and connectivity. Fueled by an award-winning research team, Intel Security invests heavily in developing innovative products that empower home users, businesses, service providers, and public sector entities around the world to protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. We also co-founded the Cyber Threat Alliance with other security vendors to facilitate deeper industry cooperation and collaboration on cyber threat sharing and intelligence. This has in turn allowed alliance members to deliver better security to their customers—from large enterprises to small businesses to home consumers.

Combining Intel's decades-long computing design and manufacturing experience with Intel Security's market leading cyber security 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 changes every day with each new technology that is brought to market. 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.

THE INTERCONNECTED THREAT LANDSCAPE

Increasing Sophistication of Attackers Threatens Organizations of Every Size. Over the past decade, attackers have evolved from recreational "hackers" with limited capabilities to organized crime and state-sponsored actors 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.

The attacker community has matured enough to support a vibrant criminal underground economy. Online web stores now sell hacking tools to any would-be attacker, and online markets make it easy and efficient to sell stolen credit card information. Attackers are also busy developing new techniques that are substantially more difficult to detect and stop, setting their sights beyond the operating system or applications and instead focusing on the underlying virtual machines, firmware, and hardware. The growing sophistication of these tools and methods of attack has unsurprisingly placed a tremendous amount of pressure on today's security processes, tools, and people.

Innovative Technologies Bridge Resource Gaps for Public and Private Sector Organizations, But Also Magnify Threats. It should come as no surprise that cyber criminals closely follow the latest technology trends because that's where the targets are the most promising. Technological innovations can help organizations deliver better overall security and operations, but can simultaneously expose new avenues for attack, such as:

Mobile Threats: All organizations are relying more on mobile devices to improve communication and business processes, and this trend will undoubtedly continue. At the same time, malware written specifically to attack mobile devices is proliferating, creating new challenges as organizations attempt to secure mobile as well as traditional compute platforms.

Migration to the Cloud: Organizations can reduce costs, improve offerings, eliminate complexity, and reduce reliance on onsite technical staff by outsourcing their IT and communications systems to the cloud. At the same time, however, they must be careful not to sacrifice security to achieve these new efficiencies.

IoT and the Explosion in Number of Devices: The exponential increase of Internet-enabled and networked devices known as the Internet of Things (IoT) is expanding both risks and rewards. Organizations are using networked metering devices, sensors, appliances, and point of sale systems to deliver better customer service and streamline business processes, but must also be aware that many IP-enabled devices were not designed with security in mind and could introduce unnecessary risk to vital IT networks and systems.

Bring Your Own Device (BYOD) Environments: Given the mobile nature of today's workforce, as well as the increasing use of BYOD programs, employees at companies of all sizes commonly access organizational resources from external networks such as hotspots and home networks. The result is often that company-owned network equipment will be simply unable to inspect the growing amount of traffic and devices connected to internal IT networks.

Traffic is Encrypted: Even when accessible, application and web traffic are increasingly encrypted. This is often done with better security in mind but may also mean that network security devices are unable to inspect traffic content for hidden threats.

Performance Issues Preempt Security: Customers are increasingly choosing to forego bulkier security features like firewalls in favor of maximizing network performance levels, creating a tug-of-war between security and performance priorities.

Adversaries Enjoy Significant Advantages. Our research and analysis reveals that cyber adversaries benefit from and exploit several key advantages, including:

- The ability to quickly enhance the tools and capabilities used in an attack through a community of innovators and service providers. This has an outsized impact on small organizations, who may not have the resources to deploy the latest adaptive technologies, or are not deploying risk management-based solutions at all.
- A working knowledge of how organizations implement defenses, including knowledge of specific product deployment models, industry architectures, and even specific vulnerabilities. While an attacker only has to be right once, organizations must be impenetrable 100% of the time—a statistic that is unrealistic even for the most well-resourced security vendors or large corporations.

ENGAGEMENT IN PUBLIC PRIVATE PARTNERSHIPS

Individuals and organizations across the spectrum cannot manage their protective defenses alone; it is a shared threat 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:

- **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 expertise to advance the rapid adoption of secure technologies around the country. In addition, we remain actively engaged in the development of new cybersecurity 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.

PRESIDENT'S CYBERSECURITY NATIONAL ACTION PLAN (CNAP)

Intel believes that good security is the result of strategic and generous investment in the three-legged stool of **technology, process, and people**. Weakness in any of these three legs will quickly undermine an organization's ability to protect itself in today's threat environment. Accompanied by a 35% increase to federal cyber budgets, the president's Cybersecurity National Action Plan encourages deeper public-private partnerships and represents a substantial investment in all three legs of the stool. As such, we support and applaud the CNAP and its work to advance the fundamental precepts of strong cybersecurity and privacy.

Specifically, the CNAP supports the **technology** leg of the stool with a $19 billion investment in federal cybersecurity budgets, in addition to a $3.1 billion Information Technology Modernization Fund to retire and replace many aging federal IT systems still in operation. Importantly, the Plan also seeks to leverage the power of public-private partnerships on efforts like the Linux Foundation's Core Infrastructure Initiative, which seeks to secure internet "utilities" like open-source software and standards, and will result in better interoperability among commonly-used security capabilities.

At a broader level, the updated 2016 Federal Cybersecurity R&D Strategic Plan ensures continued focus on longer term opportunities for industry, government, and academia to collaborate on technological and systems innovation to keep pace with evolving threats. Finally, CNAP asks government and industry to jointly develop a Cybersecurity Assurance Program to test and certify networked devices within the "Internet of Things," whether they be refrigerators or medical infusion pumps. Intel firmly believes that global, industry-led security standards and best practices will be key to the program's ability to achieve its objectives.

The CNAP strengthens the **process** leg of the stool by encouraging the creation of federal capabilities like the National Center for Cybersecurity Resilience, which would enhance the development of accurate and repeatable processes to assess and mitigate system vulnerabilities in private industries. The CNAP further supports strong cyber processes through the administration's commitment to developing and implementing international cyber norms, allowing American companies to operate with more predictability and assurance in a global economy. The Plan also seeks to expand awareness of good cyber hygiene and more effective security processes by leveraging the National Cyber Security Alliance (NCSA) and engaging the private sector to assist in the widespread adoption of multifactor authentication technologies. Intel serves on the board of the NCSA and is committed to supporting the expansion of the "Stop.Think.Connect." awareness campaign to achieve this vital objective. Recognizing the importance of privacy to creating strong security processes, the Plan's establishment of a Council of Federal Privacy Officers shows leadership and an awareness of the things that matter to the security and vibrancy of Americans' digital lives. Efforts like these are key to advancing the best practices and security management processes that organizations of all sizes need in order to maintain appropriate security and privacy controls and governance.

Finally, and of particular interest to Intel Security, is the **people** leg of the stool. The CNAP takes important steps to reverse the cyber talent shortage with the inclusion of a $62 million increase to the President's Budget to bolster cybersecurity personnel programs. As one example, the Plan would establish the CyberCorps Reserve program, providing cyber education scholarships to Americans seeking to serve their country in the federal civilian government. Other examples include the development of a Cybersecurity Core Curriculum, an increase in the number of participating academic institutions in the NSA Centers for Academic Excellence in Information Assurance Education program, and an expansion of student loan forgiveness programs for cyber professionals joining the federal workforce.

These education and workforce investments, in particular, will make a vital down payment to help close the cybersecurity skills gaps in government and the private sector. With more than 209,000 cybersecurity jobs in the U.S. unfilled last year, and predictions of 1.5 million more cyber jobs than takers by 2019, Intel is committed to supporting the CNAP's cyber workforce efforts and expanding initiatives like the CyberCorps Reserve program. The CNAP is a great step forward, but to remedy our alarming cyber talent deficit, we must recruit more than a million Americans trained in cybersecurity and information assurance. Only the federal government can lead the response. By offering young STEM graduates immediate employment protecting government and other critical assets, the government could stand up a Cyber National Guard that would quickly produce a trained workforce with practical experience and security clearances. After serving their country for five years in the public sector, they would find private companies like Intel eager to hire them – and pay them what they are worth.

While the CNAP contains many significant investments in **technology**, **process**, and **people**, we would also encourage additional investment at the state and local levels. As cybersecurity concerns are equally urgent at other levels of government across the country, it is imperative that additional resources and grant programs be leveraged to strengthen the cyber capabilities of under-resourced governments. Additionally, while industry can develop new security technologies and take steps to safeguard our own networks and information, only the government can prosecute cybercriminals and enforce critical legal frameworks across national borders. Given the global nature of our digital infrastructure, we need government to further invest in a global law enforcement network capable of delivering justice anywhere a cybercriminal or terrorist resides.

RECOMMENDATIONS FOR THE PRESIDENT'S COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

Intel believes that the government is most helpful when it leads by example, convenes key stakeholders, and adequately invests in infrastructure security through acquisition, education, and R&D. Through the president's Commission on Enhancing National Cybersecurity, the CNAP created a useful venue for industry leaders and experts to identify additional areas in need of investment and new opportunities for public-private engagement.

As it prepares to issue its first report in December, we urge the Commission to keep the following principles in mind:

1. Assess existing collaborative work before making new recommendations. More than another strategy document, policymakers need a clear roadmap for strategy execution and deliverables. This will support a seamless transition from the current administration to the next, while taking stock of past successes and areas for improvement.

2. Reinforce the consensus around voluntary, non-regulatory, public-private partnerships and best practices to support such vital initiatives as real-time information sharing and industry-led, global standards-setting processes.

3. Recognize that technology mandates such as government imposed back-doors chill innovation, hurt the economy, and weaken security. The technology industry is fast-moving and relies on rapid innovation to meet customer requirements and address constantly evolving cybersecurity risks.

4. Prioritize paying down the "cyber debt" and reversing the current talent shortage. In particular, we recommend expanding initiatives like the CyberCorps Reserve program and standing up a Cyber National Guard to train and recruit new talent and protect public and private digital infrastructure.

5. Recommend additional incentives and governance models to drive uniform federal cybersecurity management and interoperable solutions that scale to meet the needs of the federal enterprise. Government-wide efforts of this kind will help lead by example and support similar initiatives in the private sector.

6. Invest in additional broadband to enable the hyper-connected network of cyber-physical devices and systems that make up the "Internet of Things (IoT)" and Industrial Internet. In the interest of global competitiveness and IoT security, safety, and privacy, the Commission should consider investments in our nation's IoT infrastructure beyond a 10-year time horizon.

CONCLUSION

I would like to once again thank this distinguished panel for giving me the opportunity to discuss Intel's approach to an increasingly interconnected threat landscape, as well as the aspects of the CNAP that we hope will strengthen existing public-private partnerships and enhance our national cybersecurity posture in the digital age. We firmly believe that effective public-private collaboration offers our best 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 and improve cybersecurity at the international, state and local levels. Paying down this "cyber debt" will require both industry and government to step up and make hard choices. Intel looks forward to continuing our engagement on these matters through our involvement in public-private partnerships and investments in **people**, **technology**, and **process**.

BIOGRAPHY

Patty Hatter

VP/GM – Intel Security
Professional Services
Intel
Patty.Hatter@Intel.com

Patty Hatter is vice president and general manager of the Intel Security Group Professional Services organization. She recently transitioned from the role of Intel Security CIO, and prior to that was the vice president of Operations and CIO at McAfee. She has overall responsibility for leading the Professional Services organization and expanding Intel Security's Consulting, Managed Services, Deployment and Training services.

Patty has more than 25 years of experience leading operations and technology organizations at several Fortune 500 companies. She joined the Intel organization in 2011 with the acquisition of McAfee Inc., now a wholly owned subsidiary that operates as the Intel Security Group. As vice president of operations and CIO at McAfee, Patty orchestrated a global transformation of IT and operations, turning the team into an asset that supported the broader enterprise-wide cost savings and revenue growth initiatives across McAfee.

Before joining McAfee in 2010, Patty was vice president of business operations at Cisco Systems Inc. She was responsible for improving integration between Cisco's processes and systems, with the company's sales channels. Earlier in her six-year tenure at Cisco, Patty led a transformation of the company's global processes and systems infrastructure that contributed to growth, scalability and revenue. She started her career at AT&T Inc., where she spent 15 years holding various leadership roles in strategic planning, business development and professional services within the United States and Europe.

Patty earned bachelor's and master's degrees in mechanical engineering from Carnegie Mellon University. She currently holds multiple advisory board positions, and is also a board member for the Silicon Valley Education Foundation.

.