STATEMENT FOR THE RECORD OF

SCOTT MONTGOMERY, VICE PRESIDENT & CHIEF TECHNICAL STRATEGIST,

INTEL SECURITY GROUP

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES CYBERSECURITY AND INFRASTRUCTURE PROTECTION SUBCOMMITTEE

ON THE CURRENT STATE OF DHS PRIVATE SECTOR ENGAGEMENT FOR CYBERSECURITY

March 9, 2017 10:00 AM | HOUSE CAPITOL VISITOR CENTER (CVC) ROOM 210

Good afternoon, Chairman Radcliffe, 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, Intel Security Group, part of Intel Corporation.

I am pleased to address the subcommittee on the value and effectiveness of current private sector engagement with the Department of Homeland Security (DHS) given its importance in helping DHS achieve its mission of enhancing the security, resilience, and reliability of the nation's cyber and communications infrastructure. My testimony will address Intel Security's commitment to cybersecurity, our assessment of the global threat environment, the state of various DHS public-private partnerships and private sector partnership innovation. Finally, I will make a number of public policy suggestions to help the new Administration shore up the capabilities and effectiveness of DHS public-private partnerships.

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 of experts that carry 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 SECURITY'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, Intel Security brings 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 with each new technology that is brought to market at a faster pace than ever before. The sharp rise of internet-enabled devices (known as “Internet of Things” or “IoT”) in government, industry and the home exacerbates this already difficult challenge. The challenges we face are too significant for one company or entity to address on its own. Real change on cybersecurity requires leadership from Washington, DC, and a true public-private partnership with industry.

Collaboration will be the driving force behind what soon will be the new McAfee (currently known as Intel Security) —planned to be a standalone company this year. It’s also why 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.

To be successful, it is 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. 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 to 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. Such technology can be guided by the strategic intellect that only humans can provide. Thus, the only way to have a winning cybersecurity strategy is to bring technology, the cybersecurity industry and the efforts between government and the private sector together. This is what real collaboration is all about.

As we collaborate with our public partners, it’s important to highlight how the threat landscape has changed over the years. It’s a top-tier issue for government leaders because of the critical role IT systems play in our national security, economy and daily lives.

THE INTERCONNECTED THREAT LANDSCAPE

Increasing Sophistication of Attackers Threatens Organizations of Every Size

The threat landscape is ever-changing, and it's getting only more complex with the sharp rise in internet-enabled devices (IoT) and industry's shift to new computing paradigms such as cloud computing. What we call the "attack surface" continues to grow. This means that organizations – and more importantly, individuals – are now more vulnerable in more places. Adversaries are increasingly capable of attacking strategic assets and critical infrastructure. Traditional platforms such as phones, tablets, laptops and servers continue to be high-value targets, but we must expand our thinking to include all devices that are "smart" and connected. Modern computing runs our factories, flies our planes, drives our cars and runs our homes. Almost every aspect of what our country runs on is potentially vulnerable to a cyber-attack.

The attacker community has matured enough to support a vibrant criminal underground economy. Online web stores on the "Dark Web" now sell hacking tools to any would-be attacker, and online markets make it easy and efficient to sell stolen credit card and other personal 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 computing 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 IoT 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.

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 enhance the tools and capabilities used in an attack quickly 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.

INTEL SECURITY'S VIEW OF PUBLIC PRIVATE PARTNERSHIPS

Our Commitment to the Partnership Model

Given the current cybersecurity threat environment, 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 cyber-attacks, and they thrive on sharing threat indicators, best practices and incident response in a mutual, non-regulatory environment.

Intel and Intel Security have been active in public-private partnerships managed by DHS and other agencies for more than 10 years. We have leadership roles in the President's National Security Telecommunications Advisory Committee (NSTAC), Information Technology Information Sector Coordinating Council, Information Technology Information Sharing and

Analysis Center, National Cyber Security Alliance and National Cybersecurity Center of Excellence (NCCoE). Through these partnerships, Intel Security 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 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 the public-private partnership model will continue to protect and serve our national interests well into the future. However, public-private partnerships, as any partnership, benefit from regular reviews, gap analyses and a commitment to continual improvement.

Policy Recommendations to Improve Public-Private Partnerships

1. **Move to Real Time Threat Information Sharing**

The Administration needs to solidify its information sharing strategy. Sharing threat information has been a necessity since I started in cybersecurity, yet we still are not focused on sharing threat information that will provide real benefits in a meaningful way. With the passage of the Cybersecurity Information Sharing Act (CISA), DHS was directed to deploy the Automated Indicator Sharing (AIS) program. This program allows both the private and public sectors to share indicators of compromise (IOC) and mitigation with each other. CISA also does an admirable job of requiring companies and government agencies to strip out personal identifiable information (PII) and put in place thoughtful processes and policies to protect citizen privacy.

While the overall program has been a strong step in the right direction, it still provides far too little real value. IOCs are just the breadcrumbs that network security staff look for to uncover clues as to what may be occurring inside their organizations. Typical IOCs are registry keys, MD5 hashes of potential malware, IP addresses, virus signatures, unusual DNS requests, URLs, etc. While these can be useful, they are really not enough to provide the defensive information needed to protect an organization. Today, AIS does not provide a means for enriching the information it shares. It simply shares minimal IOC information.

To defend our institutions properly, defenders need to understand cybersecurity threats and their components as a whole. Indicators, incidents, tactics, techniques and procedures used, threat actors, associated campaigns, what is being targeted, malicious tools being used, software vulnerabilities being exploited, courses of action to mitigate the threat, are all components of a cyber threat that need to be understood. Instead of trying to share simple breadcrumbs, we need to be sharing with a focus on providing a platform for enriching specific threat information so we can see and understand more about the threat.

Often one company may discover an IOC, another may be able to associate it with a specific vulnerability, and still another may be able to provide a correlation between the known threat items and a past or similar attack that could lead to a potential remediation, thus mitigating the threat. Today we have no way to share enriched threat data effectively. We need information sharing with a focus on enhancing our abilities to protect our organizations. The Administration should double down on working with the private sector to further evolve the way cyber threat information is represented, enriched and distributed in a timely fashion. Cyber criminals are excellent at information sharing; the government and private sectors must be as well.

2. **Encourage Full Utilization of and Update Government Procurement Rules to Enable DHS to Compete with Hackers**

There are significant gaps at DHS that preclude it from competing with hackers, cyber criminals and other bad actors who innovate and share information quickly, often using state-of-the-art technology. Thus, it is critical that DHS and other federal agencies have access to the same tools. This can only be achieved by encouraging full use of current procurement rules, and by looking for opportunities to update those rules where necessary. Currently, there are five ways federal agencies can acquire products and services rapidly:

- Under the Federal Acquisition Streamlining Act of 1994 (FASA), Congress mandated, to the maximum extent practicable, the use of simplified acquisition procedures (SAPs) for products and services not exceeding the simplified acquisition threshold.
- The Competition in Contracting Act of 1984 (CICA) allows federal agencies to accelerate the acquisition process where there is an urgent need, or where requiring full and open competition could compromise national security.
- The U.S. General Services Administration (GSA) maintains a supply schedule for information technology (Schedule 70), where pre-vetted vendors with pre-negotiated terms offer cybersecurity products.
- Congress authorized the Continuous Diagnostics and Mitigation (CDM) program at DHS, which allows federal agencies to expand their CDM capabilities through the acquisition of commercial off-the-shelf tools, with robust terms for technical modernization as threats change.
- Congress has granted 11 agencies (including DHS) the ability to enter into "other transaction agreements," which generally do not follow a standard format or include terms and conditions normally found in contracts or grants, in order to meet project requirements and mission needs.

In addition to encouraging federal agencies to fully use these procedures, procurement policy and acquisition procedures must evolve more rapidly to match the pace of information technology development and adoption by hackers, criminals and other bad actors. Currently, little guidance exists in the Federal Acquisition Regulations (FAR) regarding the procurement of cybersecurity technology; rather, the FAR leaves cybersecurity implementation to each

individual federal agency. Agency officials and contractors must consult a myriad of different agency regulations to ascertain if and how other agencies have implemented their acquisition regulations regarding cybersecurity. This diversity in agency cybersecurity regulations undermines security requirements and policies governing federal procurements. Harmonizing cybersecurity acquisition requirements would allow agencies to: (i) target security to highest-priority data and threats; (ii) obtain greater value through reduced compliance obligations and increased contractor focus on high-value cybersecurity investments; and (iii) enhance agency cybersecurity through the adoption of best practices, tempered through public review and comment.

3. Create Additional Incentives to Participate in Information Sharing Partnerships:

A critical provision of CISA is that it gives liability protections to private companies that share cyber threat information (CTI) and defense measures (DM) on a voluntary basis with DHS. Recent guidance from DHS on CISA clarifies that private entities also receive liability protection under section 106(b) (1) for sharing CTI and DM information with other private entities. Policymakers have done an admirable job of using the incentive of liability protections, and relaxing antitrust rules, to help incent broad-based information sharing between the private sector and the government, and among private sector entities. However, too few companies are actively sharing threat information with DHS and among themselves to fully realize the aim of CISA – a high functioning eco-system of information sharing that enables the public and private sectors to compete with global networks of sophisticated hackers.

We need to recognize the disincentive that threat intelligence's "free rider" problem has imposed on public and private sector information sharing. Every organization benefits from consuming threat intelligence but gains no direct value from providing it unless the right organizational structure and incentives are put in place to eliminate the free rider problem.

While DHS has made progress, it still needs to improve the quality and the quantity of the threat data it shares with the private sector to address this issue of the free rider. DHS should thus declassify larger categories of threat data and actively share them with the private sector. DHS should issue many more security clearances to qualified company representatives to enable access to the most sensitive, and potentially most valuable, pieces or classes of threat data.

Finally, the new Administration should pass into law The Cyber Information Sharing Tax Credit Act – sponsored by Senators Moran and Gillibrand – that would incentivize businesses of all sizes to join sector-specific information sharing organizations, known as Information Sharing and Analysis Centers (ISACs), by providing refundable tax credits for all costs associated with joining ISACs. The effort should not just focus on ISACs but should also include Information Sharing and Analysis Organizations (ISAO) as well. ISAOs are not limited to individual critical infrastructure sectors as ISACs are, and they allow diverse organizations to share cyber-related threat information.

4. **Use the NIST Cybersecurity Framework Process as a Model for Public-Private Partnerships**

The Framework for Improving Critical Infrastructure Cybersecurity, known as the NIST Cybersecurity Framework, is widely acknowledged as a highly successful model of public-private partnership. The Office of Management and Budget is already working to encourage federal agencies to adopt the Framework, the new Administration's draft executive order mandates government agencies to deploy the Framework, and the private sector is rapidly adopting it. Here's our analysis of why:

- The need was real
- The process was open
- NIST listened first
- They were prepared
- They engaged all stakeholders
- The framework was voluntary – not regulatory

I'd like to expand on each of these aspects, not simply to compliment NIST but to offer the process as a model for future public-private partnerships.

The need was real

PPPs created around a topic or issue that is real to both the public and the private sectors has a much better chance of getting the exposure and participation needed to achieve the goal of the partnership. In the case of the Cybersecurity Framework, it was obvious to both groups that the need existed. While NIST had a hard timeframe to be successful in – one year-- they had a long history in risk management and understood the need well. For too long regulatory compliance had forced industry to spend valuable security dollars to prove something to the regulators instead of using those resources to help protect enterprises. The cost of compliance was impacting our ability to secure ourselves.

Openness of the process

From the very beginning, NIST made it clear this was going to be a very open process. In the initial meeting, NIST staff described what would be occurring, from the RFI-submitted comments being made public on a NIST project website, to the anticipated workshop process and general timeline for various milestones. Along the way, NIST staff were quick to ensure that industry participants understood what was happening so there would be no surprises. This created a growing sense of trust as the effort evolved and made the process more effective during the development of the Framework.

Listening

One of the more interesting and effective parts of the development was the way NIST staff listened to the workshop participants. They used a moderated dialog approach that allowed all

attendees to voice their opinions to a set of topics the NIST staff wanted to learn about. There were very active discussions that were highly informative from members of various sectors and industries. Dr. Gallagher, NIST's Director at the time, stated quite clearly this was not NIST's Framework; this was the community's Framework. Having the public side of a public-private partnership listen instead of dictate allowed private sector participants to voice their opinions in a much more open and direct way. This too built trust as the effort went along.

Being prepared

Each of the workshops seemed very well organized, and the topics, panels, questions and outcomes were well thought-out before each workshop began. This gave participants reassurance their time was being well spent. Open forums with no direction or planning do not give those involved much confidence the effort will succeed. Being prepared also meant participants needed to do their homework as well. While not always the case, as the workshops advanced, they did so.

Engaging all

One of the smartest things NIST did as part of the Framework development process was to understand they needed to get outside the Beltway for the effort to be successful. They held the workshops in different locations around the country so the local owner/operators of the critical infrastructure could have their voices heard. This ensured there was a diverse group at each of the workshops and all were able to participate. The processes used during the workshops encouraged all in the room to contribute and they did. A highly interactive, collaborative environment is one where real dialog can occur and produce positive results.

Voluntary, non-regulatory nature

The fact that NIST is a non-regulatory body also helped their credibility and the private sector's attitude towards participating and contributing. This was a topic area that had a lot of people concerned initially, but as the effort progressed, more and more private sector participants relaxed and believed in the voluntary intent of the effort. NIST also made it clear in each workshop that they were requiring a non-attribution from any and all regulators in the room. Each agreed to the rules, making it much more comfortable for real open and honest dialog to occur.

While others have tried to copy the NIST success, often they have left out one or more of the characteristics that made the Cybersecurity Framework effort a success. In reality, both the public and the private sector participants must buy in. To do so requires trust in the process, the effort and the vision for the outcome to be successful

5. Seek Innovative Ways to Further Grow the Information Sharing Eco-System

Company to company information sharing is growing in certain parts of the economy. An example is the Cyber Threat Alliance (CTA). Intel Security, along with Check Point, Cisco,

Fortinet, Palo Alto Networks and Symantec, worked together to start and build the CTA. This is a group of cybersecurity practitioners from organizations that have chosen to work together in good faith to share threat information for the purpose of improving defenses against advanced cyber adversaries across member organizations and their customers. The key to the success of this effort is that each organization must supply threat information to all the members in order to receive threat information. This allows each of the member organizations to incorporate the others' threat information into their products' protection mechanisms. This is an example of valuable and actionable shared threat information having a direct and positive impact on improving their customers' environments. The member organizations have decided to participate in the Alliance for the betterment of the ecosystem they serve.

The CTA is also showing that with the right organizational construction – with the right incentives to collaborate – real progress in private sector information sharing can be made. Examples of successes include cracking the code on Crypto Wall version 3, one of the most lucrative ransomware families in the world, totaling more than US $325 million ransomed. CTA's disruption of Crypto Wall 3 forced cybercriminals to develop Crypto Wall version 4, which the CTA also uncovered and resulted in a much less successful attack. This is a prime example where creating an operationally holistic view of the threat and how to address it has had an extremely positive impact on our ability to protect ourselves.

To further incentivize companies to share threat information among themselves, policymakers should amend The Cyber Information Sharing Tax Credit Act. Such an incentive would help speed the growth of existing private sector to private sector information sharing coalitions and help start news ones, particularly in some sectors of the economy that have been slow to realize the benefits of sharing threat information with partners and competitors.

CONCLUSION

Given the rapidly changing threat environment, public and private sector organizations cannot go it alone. The challenge is never-ending, but I have no doubt that the public-private partnership model will continue to protect and serve our national interests well into the future. Public-private partnerships benefit from regular reviews, gap analysis and a commitment to continual improvement. The subcommittee should be commended for taking such a thoughtful approach to reviewing the successes and challenges of DHS managed public-private partnerships.

As stated earlier, DHS deserves much praise. It manages a thriving number of public-private partnerships that serve the national interest. At the same time, real time information sharing needs to be implemented on a grand scale, IT procurement rules should be updated, DHS partnerships need to be benchmarked against other successful ones on a regular basis and additional incentives should put in place to help grow the information sharing eco-system. Intel Security – soon to become McAfee – is committed to continue to invest, engage and contribute

to support the long-term success of the partnership model. Our collective security depends on making the promise of “together is power” a reality.