Written Testimony of:

Major General (Ret.) John A. Davis, U.S. Army
Vice President and Federal Chief Security Officer, Palo Alto Networks

Before the:

U.S. Senate Committee on Armed Services
Subcommittee on Cybersecurity

Regarding:

"Department of Defense's Cybersecurity Acquisition and Practices from the Private Sector"

November 14, 2018

Chairman Rounds, Ranking Member Nelson, and distinguished members of the subcommittee, I am honored to appear before you today to discuss innovation in the commercial cybersecurity industry and the ways in which the U.S. Department of Defense (DoD) could apply these innovations to advance its own cybersecurity posture. I want to first thank you for your leadership on this issue, and offer my commitment to work in partnership with you and your staff to support this Committee's continued oversight responsibilities as we collectively seek to bolster the Department's and Nation's cyber defenses.

The Department deserves credit for its efforts to modernize and improve the security of its information technology infrastructure, especially by leveraging commercial technologies and the benefits of the cloud. My comments today are designed to help DoD improve in the following areas by focusing on desired outcomes: Increase the **speed** of defending against an increasingly agile cyber threats to DoD's missions; **scale** the ability to prevent successful cyber attacks against a growing and continuously changing set of mission critical systems, networks, devices and operating platforms; and improve **trust in the security and capability** of the technology procured to accomplish the defense of DoD's information networks and operational technology.

These outcomes are possible today and here are the key points that I wish to reinforce about how a strong partnership between DoD and industry can drive towards achieving them:

- Innovation in the commercial cybersecurity industry is heavily focused on software-based machine learning, automation, and seamless "platform" integration. This provides continuous and consistent threat visibility and the delivery of automated protections across the entire enterprise environment, from network to cloud to endpoints and even operational devices connected to the network. The network defender's goal should be to bring software to a software fight, and to use advanced analytics and effective cyber threat information sharing partnerships to change the current imbalance between attackers and defenders.

- DoD is taking good steps to incorporate commercial innovation but could enhance its efforts by better aligning procurements to mission-owner needs through a "DevSecOps" model of operational testing and evaluation, and by creating incentives for companies to adopt best practices in areas like supply chain risk management. (DevSecOps is a term in the technology world that transforms the traditionally segregated functions of software development, security and operations into agile, continuously reinforcing cycles where each function is natively integrated with the others through rapid parallel process instead of a lengthier sequence of separate steps.)

Before I expand on these key points, I would like to introduce myself and my company.

I am a retired U.S. Army Major General now serving as Vice President and Federal Chief Security Officer for Palo Alto Networks, where I am responsible for expanding cybersecurity and global policy initiatives for the international public sector and assisting governments and industry organizations around the world to prevent successful cyber attacks.

Prior to joining Palo Alto Networks, I served as the Senior Military Cyber Advisor at the Pentagon and was appointed as the acting Deputy Assistant Secretary of Defense for Cyber Policy. Prior to this assignment, I served in multiple leadership positions in operational cyber assignments, special operations and information warfare. These experiences provide me with a unique perspective on both the commercial cybersecurity marketplace as well as efforts underway at DoD to successfully leverage technological advances in cybersecurity.

For those not familiar with Palo Alto Networks, we were founded in 2005 and have since become one of the world's largest cybersecurity companies, with a mission to protect our way of life in the digital age by preventing successful cyber attacks. We serve more than 54,000 corporate and government enterprise organizations in more than 150 countries worldwide. We support 85 of the Fortune 100 and more than 63% of the Global 2000 companies, are partnered with elite technology leaders including Amazon Web Services, Google, and Microsoft, and were named to *Fortune* magazine's Top 50 companies changing the world and Future 50 lists.

Palo Alto Networks collaborates extensively with key stakeholders across the U.S. Government executive branch and with like-minded countries internationally. This includes our membership on the President's National Security Telecommunications Advisory Committee (NSTAC), which brings industry executives together to provide counsel on national security policy and technology issues for the President and other senior U.S. government leadership. We also have formal executive branch partnerships to test our innovative cybersecurity technologies based on government mission needs, and we share cyber threat information with the Defense Department, other executive branch agencies in the civilian, law enforcement, and intelligence communities, international partners including NATO, and with private industry partners.

Innovation in the Commercial Cybersecurity Industry

I would like to begin by recognizing a paradox of the security marketplace. Broadly, our digital world is getting simpler and easier to use, more connected by design, with automated functions requiring fewer people to execute: overall, more *convenient* for the user. Just consider how you use your smartphone in a way that was unthinkable a decade ago. On the other hand, the security world is producing more products operating in individual silos without regard for other security products and continuing to rely on human decision making and manual response: overall, *slower, less efficient, and more complex*.

The key innovation in the cybersecurity marketplace will be to reverse this trend.

To do so requires an understanding of the adversary's tactics and techniques, and the steps network defenders can take to see and stop them.

The adversary: The cybersecurity community has significant insight into the basic steps that any cyber actor or organization uses to accomplish a successful attack, known as the "attack lifecycle." These steps include reconnaissance, a mechanism to get into a target, exploitation of some vulnerability within the network, installation of malicious code, establishment of a control channel, escalation of access, and then lateral movement within a network environment. The final step in this process, defined as a successful attack, can result in exfiltration of sensitive information, encryption of data for ransom, disruption, degradation, destruction, deception, or even the public exposure of embarrassing information. Understanding the attack lifecycle means that the attacker must be right at each step to be successful and the defender only has to see and stop the threat at any one place along the process in order to prevent a successful attack. With this mindset, we can help to flip the equation in favor of the defender and achieve cyber threat prevention.

Today's environment overwhelmingly favors the attackers. As the cost of computing continues to decline, our adversaries have been able to conduct increasingly automated, successful attacks at minimal cost. In fact, many free and open source tools are available online that enable repeatedly successful attacks against poorly defended networks.

In the face of this automated onslaught, the network defender is generally relying on legacy security technologies, often cobbled together as multiple layers of "point" products that solve discrete problems but do not interoperate in a way that can reduce priority risks across an organization's entire network infrastructure. This increased technological complexity creates a dependence on people – one of the least scalable resources in any organization – to manually defend against automated, machine-generated attacks. Network defenders are simply losing the economics of the cybersecurity challenge because they are bringing people to a software fight.

To flip this equation and gain back leverage against our adversaries, we collectively need to embrace integrated approaches that simplify and automate network defense.

To prevent successful attacks, four key functions help a defender maintain advantage in our increasingly complex and dynamic network environment.

1. *Gain Complete Visibility*. You cannot stop what you cannot see, and you must gain complete visibility of your entire network environment, including mobile devices and the cloud.
2. *Reduce Attack Surface*. You must identify the systems, networks, data and even people that are critical to your business or mission and prioritize your security efforts around them. You should segment your environment to simplify your ability to see threats and enforce security controls and to ensure that, if there is a breach, it is limited in scope and consequence to the business or mission. Additionally, you must create a "zero trust" network environment where only authorized users are allowed to conduct authorized functions, using authorized applications with authorized content. Everything else must not be permitted unless by exception.
3. *Stop Known Threats*. You must stop all known threats associated with each step of the attack process.
4. *Discover Unknown Threats Quickly and Stop Them*. You must identify unknown suspicious behavior, analyze it quickly using machine learning, decide whether it is malicious, and enforce a security decision to prevent it.

The Palo Alto Networks perspective on preventing successful cyber attacks is built on four levels of innovation that leverage automation through capability integration, advanced analytics and improved cyber threat intelligence sharing to change the current imbalance between attackers and defenders.

The first level of innovation is about using a **platform approach** to automate the establishment of visibility and security controls at each point along the attack process. In a platform, processes are all automated and capabilities are designed from the beginning to communicate with each other across each of the variations within an organization's network environment. This is a comprehensive and purpose-built package approach instead of a loose collection of bits and pieces that are cobbled together and bolted on as an afterthought. The distinction results in a comprehensive, continuous and consistent ability to see and stop threats before they are successful as opposed to looking through soda straws at discrete portions of your network environment and lacking the ability to correlate events that identify a threat attack in process.

The core benefit is consistent visibility and protections to see and stop threats before a successful attack outcome can occur. For instance, we build technology that identifies new threats at the key tactical places where cyber attackers need to take action to be successful. As a result, we generate more than 1.6 million new preventive measures each week that are automatically deployed within minutes to protect our customer base. A platform approach is easier to use, more convenient for the consumer, requires fewer people to do more things, and is designed to prevent most threats.

The second level of innovation is **strategic partnerships**. In my opinion, there is no single entity in either the public or private sectors that can secure across the various network environments (physical, virtual, mobile, and cloud) in isolation. Integration at this level in industry requires deep technical partnerships between companies who are best in breed at what they do within the different portions of the network enterprise environment where the various cyber threat attack process steps occur. This level is focused on changing the cybersecurity market trend of an increasing number of point solutions that don't communicate with each other and are "bolted on" as an afterthought—and moving towards technologies that are better connected and natively designed to work together from the start.

Innovation at this level requires cultural adjustments in the business community as well. Effective competition in the market place has traditionally demanded that a company delivers the best individual product for the best price. To take advantage of this level of integration, security companies must now demonstrate a new key performance parameter. They must show their solution is an integrated component of a broader platform approach, and that it is technically engineered to do so natively to make it less complex for human network defenders to understand and operate. They must show that it requires fewer people to do more things, aligning to trends in the technology world that cybersecurity is supposed to protect in the first place.

The third level is the driving force for future innovation across the cybersecurity industry: **expanding the scope and flexibility of software-based open application program interface (API) capabilities**. The cybersecurity industry must focus on "bringing software to a software fight." We must make it easy and inexpensive to integrate quickly. Open API takes "plug and play" innovation to a new level by providing incentives for emerging capabilities, including from startups, to quickly develop software-based capabilities that can integrate into an existing platform. By opening up an API layer on top of a massive cyber threat telemetry cloud containing indicators of threat compromise along the attack lifecycle, we believe the new security consumption model is to allow organizations to build their own software-based security applications, use third party apps (even from our competitors) and/or use the security apps we provide to plug into our threat telemetry and operate "security-as-a service."

The fourth level of innovation requires an overall **ecosystem of cyber threat intelligence and information integration**. Organizations that partner in effective, automated cyber threat intelligence and information sharing collectively benefit the entire community by leveraging an "over the horizon" dynamic. Whatever is seen by one organization can quickly immunize all the other organizations in the partnership, drive the costs up for cyber adversaries, and contribute to an overall deterrence of malicious cyber activities. *Industry should not compete over what they know about cyber threats, rather they should compete over what they can do with that information.* The Cyber Threat Alliance, of which Palo Alto Networks is a founding member and which includes several of the largest cybersecurity companies in the world, is a leader in this kind of innovation.

Ultimately, these innovations in the cybersecurity marketplace all take advantage of automated machine learning, bolstered by cloud technologies that enable security at scale as well as efficient training and deployment of human resources, to increase the scope and speed of identifying and preventing cyber threats.

DoD Adoption of Innovative Cybersecurity Solutions

As I noted, DoD deserves significant credit for its efforts to modernize its information technology infrastructure, and the corresponding senior-level focus on taking advantage of commercial technologies and the benefits of cloud computing. DoD has recognized that cloud-based computing will enable the Department to deploy cybersecurity measures more seamlessly and effectively. The Cloud Executive Steering Group, for instance, which reports directly to the Deputy Secretary, is a welcome strategy that will have near- and long-term benefits for mission effectiveness. However, the Department could undertake several actions to enhance its ability to make use of commercial innovations.

First, **DoD should review the requirements for its cloud-based procurements to ensure that security is considered comprehensively**. Contracts must underscore the shared responsibility between mission owners and cloud service providers. That is, while cloud service providers secure cloud infrastructure, mission owners must secure their data across all environments – across networks, endpoints, on-premise data centers, multi-cloud infrastructure, and within a single public or private cloud service provider. Contract requirements that mandate cloud infrastructure security do not obviate the need for requirements and resources also addressing the important security capabilities that mission owners must use to fulfill their own responsibilities; procurements that include comprehensive requirements for both cloud providers and security providers would provide needed clarity for all parties without penalizing bids for adding cost and complexity outside of scope.

Second, **acquisition practices must be better aligned to mission needs, through operational testing and leadership accountability**. Across the Federal government, acquisition professionals and mission owners have traditionally been separate stovepipes. Including comprehensive security requirements in contracts is important but insufficient. Accountability and incentive models for procurement officials must be oriented towards strong security and risk reduction to the agency. The current risk structure for contract officers does not map to the risk of the enterprise, often leading to lowest cost, technically acceptable bids that minimize protest risk, rather than focus on quickly putting the best performing tools in the hands of mission operators. The legacy practice of buying "bits and pieces" instead of purpose-built packages or platforms is inefficient and insecure.

One mechanism for addressing this procurement misalignment is expansion and greater use of the DevSecOps model, including utilizing real-world operational testing and evaluation programs for security technologies rather than a reliance on static requirement checklists. A key aspect of this model is decision-making that occurs at a pace that keeps up with innovation. In particular, as the Department considers the next generation of its threat detection and prevention system, DoD should use its objective operational testing ability to evaluate and rapidly deploy the most effective technology. The current system is based on years-old, hardware-based technology that has not kept up with the rapidly evolving security technology, produced in the private sector. At the same time, the hardware-based nature of the system makes it difficult to integrate next generation commercial technology from different companies easily, creating another barrier against expanding network protection to keep up with the rapidly evolving threat. It is critical that network protection move to an open, highly-scalable, commercial platform that will allow easy integration of unique capabilities while maintaining a broad base of commercial technologies that continue to evolve at the speed of the changing threat. This is even more important as the military and supporting entities move more of its capabilities to the cloud.

Procurement officials and mission owners should also consider how to take advantage of the massive repository of threat intelligence telemetry housed and shared by organizations like the Cyber Threat Alliance. I encourage DoD officials to ask companies seeking to do business with the Department whether they are members of the CTA. If not, why not?

Ultimately, contracting officials should be held accountable and incentivized to reinforce the requirement in Executive Order 13800 (*Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*) that holds agency heads accountable for managing the cyber risks of their enterprises. Agency heads can meet the Executive Order's accountability obligations by ensuring effective, independently-evaluated security requirements are built into procurement contracts, thereby aligning the incentives and responsibilities of contracting and acquisition professionals to directly support the mission owners.

Third, DoD should consider how to **create incentives for companies to adopt best practices in areas like supply chain risk management**, since the advantages of those best practices ultimately flow to the Department. This is a very effective way to increase the level of trust in the security of the technology procured and employed to defend DoD's information network and critical mission systems. At Palo Alto Networks, for instance, our design, sourcing, manufacturing, and order fulfillment processes all take place in the U.S., which offers the advantage of allowing us to more easily take steps to ensure personnel, facility and product security. DoD and private industry should work collaboratively to identify other supply chain best practices, and develop a menu of potential incentives – such as qualified bidder lists – to promote their adoption.

**

Chairman Rounds, Ranking Member Nelson, and distinguished members of the subcommittee, thank you again for the opportunity to testify today. I look forward to answering any questions you may have.