U.S. House Homeland Security Committee
Subcommittee on Cybersecurity and Infrastructure Protection Hearing:

"The Current State of DHS Private Sector Engagement for Cybersecurity"

Written Testimony of:

Ryan Gillis
Vice President of Cybersecurity Strategy and Global Policy
Palo Alto Networks

March 9, 2017, 10:00 a.m.
House Capitol Visitor Center – Room 210

Chairman Ratcliffe, Ranking Member Richmond and Members of the Committee:

Thank you for the opportunity to appear before you today to discuss how the Department of Homeland Security engages with the private sector. My name is Ryan Gillis, and I serve as the Vice President of Cybersecurity Strategy and Global Policy at Palo Alto Networks.

I would like to begin today by recognizing the tremendous leadership this Committee has shown on the issue of cybersecurity. I have seen firsthand this Committee's central role in passing a range of cybersecurity legislation that promotes responsible cyber information sharing and strengthens the Department of Homeland Security's (DHS) statutory authority to execute its mission. The Committee is directly responsible for helping shape legal clarity to expand cyber information sharing, provide appropriately targeted liability protections for companies, and establish necessary privacy protections in the Cybersecurity Act of 2015. The end result reflects this Committee's sound understanding of how critical public-private trust and cooperation is to effective information sharing, and I'm honored to support this Committee's continued oversight responsibilities. So, let me first say thank you for your leadership and for the opportunity to speak with you today.

For those not familiar with Palo Alto Networks, we have become one of the world's largest cybersecurity companies just 10 years after our first product shipped, actively preventing successful cyberattacks for more than 37,000 corporate and government enterprise customers in more than 150 countries worldwide. Our collaboration with DHS ranges from strategic policy development to operational initiatives, starting with a commitment from the top of our organization. Our CEO and chairman, Mark McLaughlin, just completed consecutive two-year terms as Chairman and Vice Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC). Founded during the Reagan Administration and administered by DHS, NSTAC brings industry chief executives together to provide counsel on national security policy and technical issues for the president and other U.S. government leadership.

Since joining Palo Alto Networks in January of 2015, my principal role has been to work with governments, companies, and organizations around the world to develop and implement strategies, policies, and operational partnerships that prevent successful cyberattacks. Candidly, this approach to cybersecurity builds naturally upon the years I spent at the DHS and on the National Security Council at the White House, and it reflects the operational reality that cybersecurity is fundamentally a shared and distributed challenge that can only be effectively addressed through collaboration, which leverages the unique capabilities and authorities of companies, individuals, and governments.

To that end, we maintain a regular cadence with appropriate government and law enforcement stakeholders around the world. The U.S. Department of Homeland Security is the cornerstone of these government engagements because of its mission to collectively prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents. Our robust and multifaceted partnership with DHS includes participation in formalized programs, as well as more informal collaboration mechanisms built on trust and personal relationships. We engage with DHS as an individual company and as part of broader collectives of private sector entities.

My testimony today will address the full spectrum of this DHS relationship, framing why public-private sector collaboration is so critical to improving our cybersecurity as a nation – and what collective actions we believe private industry and government must take to effectively leverage information sharing as a tool to achieve the desired outcome of increased cybersecurity. Finally, I'll outline specific examples of our collaboration with DHS – including information sharing, policy development, and cybersecurity exercises. In doing so, I'll highlight several tangible success stories of public-private partnerships; opportunities for potential improvements; and, not only what Congress has done to incentivize these partnerships, but also what can be done to further enable progress in these areas.

Why Public-Private Sector Cybersecurity Collaboration Is Important

Before providing an assessment of the current state of DHS and private sector cybersecurity collaboration, it is critical that we clearly define the objectives we are seeking to achieve through this partnership. As arguably the most developed mechanism of public-private sector cooperation, cyber information sharing provides a valuable use case for this discussion.

As the concept of information sharing has received widespread attention in recent years, the term has adopted an increasingly broad and varied definition. Because of this, it is critical to clearly define how Palo Alto Networks approaches information sharing, and how it fits into our broader mission of raising costs for our adversaries and actively preventing cyberattacks. This approach recognizes that cyberthreat information sharing, while critical, is not a panacea. Information sharing is one necessary tool within a much larger strategy that leverages people, process, and technology to tangibly reverse the attackers' current advantage in cyberspace.

The Palo Alto Networks perspective on cybersecurity is built on a relatively simple premise: We believe that cybersecurity is a correctable math problem that, at present, 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 discreet problems but do not interoperate in a way that can holistically 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.

To flip this equation and gain back leverage against our adversaries, we need to collectively embrace integrated approaches that simplify and automate network defense to actively prevent cyberattacks. This is a critical point: If we focus on preventing attacks in the correct locations – informed by sophisticated and integrated detection capabilities – we can deter malicious activity by making it more expensive in terms of resources, time and personal impact for our adversaries to launch a successful attack. True integration across the cybersecurity ecosystem – leveraging initiatives like automated information sharing and technology orchestration – can be the catalyst in reversing this current unsustainable dynamic that exists in cyberspace.

Our approach to automated integration begins within our own technology platform. We build technology that prevents attacks at the key tactical and strategic places where cyber attackers need to take action to be successful, and we update our global customer base with the latest protections in as little as five minutes. As a matter of scope, we generate more than 1 million new preventive measures each week as we identify new, or "zero-day," cyberthreats. This is not to imply that we – nor any one company or government – can alone see and prevent all the evolving automated threats facing network defenders. Consequently, we partner with other companies and appropriate government agencies whose competencies complement ours to help gain the leverage required to disrupt attackers and their tools.

At its core, our company's network defense and information sharing philosophy closely mirrors the ultimate vision for information sharing championed by this Committee. Our approach is focused on three primary objectives: 1) protect against all known cyberthreats; 2) turn unknown threats into known threats as quickly as possible; and 3) automatically leverage this new threat knowledge to create preventive countermeasures that are shared broadly within the ecosystem to prevent other entities from falling victim to similar attacks. This last component is critical. As this Committee knows well, information sharing is too often a time-intensive process that requires a human to read, interpret and manually create prevention controls based on technical cyberthreat indicators provided in a non-machine-readable format like a PDF or email. This manual process simply can't scale to the speed and sophistication of the modern cyberthreat environment.

Sophisticated cybersecurity companies can uniquely contribute to this challenge because we collectively have the physical infrastructure and processing ability to automatically deploy preventive measures based on new threat information to a broad customer base across multiple sectors. For these reasons, Palo Alto Networks and other sophisticated cybersecurity companies can bring a degree of actionability to information sharing that is critical for achieving our ultimate goals of raising adversary costs and tangibly improving cybersecurity across the ecosystem.

Our approach to automated integration doesn't end with our own platform or even our own company. In 2014, Palo Alto Networks was a founding member of the Cyber Threat Alliance (CTA). The CTA was incorporated in January 2017 as an independent, non-profit organization focused on cybersecurity information sharing. It is the first information sharing organization specifically among cybersecurity vendors. Michael Daniel, the former Special Assistant to the President and White House Cybersecurity Coordinator, was just appointed as the CTA's first president. The CTA now includes six of the largest global cybersecurity companies as founding members – Check Point, Cisco, Fortinet, McAfee, Palo Alto Networks and Symantec – underscoring the philosophy that we can be force multipliers in support of a coordinated threat sharing effort against cyber adversaries.

To fulfill its core mission, the CTA has built an automated information-sharing platform with the goal of enabling and incentivizing the sharing of high-quality, actionable threat information. The CTA and its platform embody a major step forward in transforming shared threat information into effective preventive measures that can automatically be deployed by CTA members to their respective customers. This isn't purely conceptual; the CTA platform is actively working to protect its members and their customers in near-real-time.

For example, recently, a single shared sample from one CTA member allowed another member to build protections before that organization's customers were targeted – preventing successful attacks against 29 subsequent organizations. In another instance, data shared through the CTA from one member allowed another member to identify a targeted attack against its customer and release additional indicators to defend that organization. The CTA and its platform have shown that a well-designed and well-built information sharing program can foster the sharing of high quality threat information among competitors, with members finding that 40 to 50 percent of shared data is new and directly actionable.

The CTA model directly addresses many of the aspects that have limited the effectiveness of other information sharing relationships, both formal and informal. First, the CTA addresses the problem of information sharing "free riders" that join information sharing groups and simply receive information without sharing. Universal contributions are achieved by establishing mandatory sharing minimums for CTA members: initially on a quantitative basis (1,000 unique cyber indicators/per day) and now evolving into a scoring system that measures the qualitative value of shared data. Second, the CTA is focused on sharing indicators related to an adversary's playbook – a more limited and predictable series of steps an adversary must take to complete a successful cyberattack. This is a key departure from many information sharing organizations, which focus instead on sharing malware samples that can be polymorphic and exist in an exponentially larger quantity than the number of unique adversary playbooks. Third, because the CTA members' collective customer base spans all industry sectors, the impact of sharing can protect a large percentage of the global ecosystem. This type of broad-based sharing of widely used threat techniques can help neutralize unsophisticated actors and force sophisticated adversaries, such as nation-states, to develop new (and therefore costlier) techniques. This narrowing of the threat landscape can make attribution easier and enable governments to more effectively target high-priority and advanced persistent adversaries and threats.

Government has a complementary and equally critical role to play in fostering information sharing across the ecosystem by leveraging its unique authorities and capabilities. DHS, for example, has the ability to amplify and distribute cyberthreat information to a wide cross-section of industry and critical infrastructure operators.

Historically, there have been many efforts by the U.S. government to more quickly declassify cyberthreat information for distribution to the broader community. However, given the rapid pace in which cyberthreats mutate and spread, the largely manual declassification process is rarely fast enough to simultaneously outpace the threat and avoid disclosures of intelligence sources and methods. Infused with a much wider set of unclassified information from the private sector, government could be able to more quickly add valuable insight and perspective without declassifying information. Leveraging the unique visibility they possess from classified information, governments can instead help direct private sector attention and resources to publicly available information on priority threats, such as nation-state activity that may target a particular sector, like energy or finance, in a way that doesn't reveal classified information.

Palo Alto Networks Engagements with DHS on Cybersecurity Issues

The Palo Alto Networks collaboration with DHS takes many forms – both formal and informal – and is related to a broad range of policy and operational activities. Operationally, our formal and informal collaboration with DHS has ranged from programmatic relationships to targeted sharing of threat intelligence reports generated by Unit 42, the Palo Alto Networks threat intelligence team. These efforts highlight threat information sharing conducted as an individual company and as a founding member of the Cyber Threat Alliance.

Cyberthreat Sharing Examples: Prior to our joining the two DHS formal sharing programs, the Cyber Information Sharing and Collaboration Program (CISCP) and the Automated Indicator Sharing (AIS) program, we established informal processes to share threats, vulnerabilities and malicious cyberthreat campaign information with DHS based on personal relationships and our knowledge of their mission and capabilities. When appropriate, we share advanced copies of significant threat reports with DHS cyber policy leadership and operational teams at the National Cybersecurity and Communications Integration Center (NCCIC). I'd like to highlight just a few specific examples of these information sharing success stories that embody the type of public-private cooperation this Committee has sought to encourage.

- In December 2016, Palo Alto Networks threat intelligence team, Unit 42, discovered new samples of Disttrack – an evolution of the same malware that was used in the August 2012 "Shamoon" cyberattack that destroyed over 30,000 hard drives at a Saudi Arabian energy company. The original Shamoon attack is widely considered one of the most significant and destructive cyberattacks in history. Prior to our report's public release, we coordinated with DHS to enable them to take preventive action. Based on several reports by Palo Alto Networks and other researchers, DHS: 1) issued two Information Bulletins to the CISCP community of network defense stakeholders, 2) updated their Indicators of Compromise (IOC) databases, and 3) created EINSTEIN signatures related to the threat to protect other federal government civilian agencies.

- In early 2016, the Palo Alto Networks threat intelligence team released a report entitled Scarlet Mimic, identifying a long-running cyber campaign targeting minority activists in China, as well as Russian and Indian government organizations responsible for tracking activist and terrorist activities. Palo Alto Networks reached out directly to DHS to share indicators related to Scarlet Mimic, allowing them to deploy preventive countermeasures across their community of network defense partners. Specifically, DHS indicated its intention to: update their Indicators of Compromise databases, vet IOCs against the intelligence community's classified databases to determine threat group attribution, create EINSTEIN signatures to protect other federal civilian agencies, and generate STIX™ files for automated distribution to their private sector CISCP partners.

- In other instances, we coordinate our outreach to DHS as part of remediation efforts with public disclosure of new vulnerabilities that our threat intelligence team discovers in publicly available technology across the ecosystem. For example, in early 2015, our threat intelligence team identified a new vulnerability in Android™ operating systems. We rapidly shared the information with Google®, so they could take steps to remediate the vulnerability, and then contacted DHS as we published the report. DHS used the provided information to generate a US-CERT alert and push the notification to their public website and their broad community of network defender partners.

- As part of the Cyber Threat Alliance, Palo Alto Networks coordinated with DHS as well as other U.S. and international government stakeholders to share threat information about CryptoWall v3 – a ransomware campaign that had extorted over $300 million from victims in under one year. Based on CTA's shared cyberthreat indicators, DHS and the FBI were able to notify victims whose websites were unknowingly compromised; contact internet service providers to disrupt compromised infrastructure; and send alerts to their network defense partners, including the international CERT community, to protect against CryptoWall v3 tactics. Subsequently, the U.S. government shared back 170 unique CryptoWall indicators with the CTA, beyond the roughly 850 indicators the CTA report initially identified. This CryptoWall example is distinct as a tangible illustration with quantifiable metrics of two-way sharing of cyberthreat information between the government and private sector.

While each of these represents an individual success story and an illustrative use case, we need to focus our collective effort on ensuring these success stories are the rule rather than the exception. We can accomplish this by continuing to build trust among partners, refining the processes, enhancing the existing sharing infrastructure, and remaining committed to automating threat sharing in a way that can effectively scale to the pace of the cyberthreats.

DHS Cyberthreat Sharing Programs: Regarding formal information sharing partnerships, Palo Alto Networks is a member of DHS's two primary cybersecurity information sharing programs: The Cyber Information Sharing and Collaboration Program (CISCP) and the Automated Indicator Sharing (AIS) program.

- CISCP is a program established to promote robust information sharing and analytic collaboration between DHS and vetted private sector partners, especially the critical infrastructure community.
- Implemented in accordance with the Cybersecurity Act of 2015, AIS is a DHS-developed

capability to enable the automated exchange of anonymized cyberthreat indicators among a wider range of private sector entities and the U.S. federal government.

AIS is intended to provide threat indicators at “machine speed” aligns directly with our efforts to increasingly automate threat sharing, as outlined above. We applaud the concept of AIS and view it as both complementary and reinforcing to the type of automated information sharing that is already responsibly occurring at Palo Alto Networks and within entities like the Cyber Threat Alliance. DHS should be commended for their continued progress in maturing these information sharing program capabilities, but there are certainly tangible opportunities for improvement.

As discussed with DHS, we believe that the administrative process for joining these programs could certainly be easier and more efficient. Because programs like AIS are dramatically enhanced by the number of contributing members, DHS would benefit from investing in resources that streamline onboarding processes and generally make these private sector-interfacing programs more customer service-focused. Specifically, DHS should develop a clear step-by-step guide for onboarding, publish those requirements broadly, and promote a singular “help desk”-type contact for all questions related to the programs. To their credit, DHS senior officials recognize these shortcomings, and plan to take concrete steps to implement personnel and process reforms that should ultimately make the AIS program more customer service-centric.

Operationally, both AIS and CISCP have initial baseline capabilities and value, but they also could benefit from incorporating best practices from industry information sharing efforts, such as the Cyber Threat Alliance’s platform. According to DHS, AIS has delivered over 218,000 unique indicators since March 2016. Additionally, CISCP published 283 Indicator Bulletins in 2016, including nearly 1,300 indicators of compromise, with a recognition they need to refine their ability to provide useful, unclassified context. However, DHS could further engage industry to leverage vendor-neutral technology and techniques that more rapidly share larger volumes of actionable cyberthreat information with context about how individual malware is used as part of broader campaigns.

Information Sharing Analysis Organizations (ISAO): Regarding cyberthreat information sharing policy development, Palo Alto Networks had a leadership role in DHS’s effort to establish and identify standards and best practices for Information Sharing Analysis Organizations (ISAO), following a 2014 presidential executive order establishing ISAOs. Specifically, our chief security officer, Rick Howard, led the effort on information privacy and security in one of six working groups that wrote and published the official ISAO standards in September 2016.

National Security Telecommunications Advisory Committee (NSTAC): Previously, I referenced our broader policy engagements with DHS, such as our CEO Mark McLaughlin’s current membership and former leadership roles in the President’s National Security Telecommunications Advisory Committee (NSTAC). Administered by DHS, the NSTAC has recently grown to become an increasingly relevant policy forum for collaboration between private industry and the U.S. government. Senior cybersecurity officials representing the White House and the Department of Homeland Security have repeatedly acknowledged the direct impact of NSTAC studies on the formulation of U.S. policy. The NSTAC has also played an important role in fostering relationships between government and the private sector technology community. For example, in mid-2016, the NSTAC hosted the first ever meeting in its 34-year history in Silicon Valley, with significant U.S. government participation, including the Secretaries of Commerce, Defense and Homeland Security, as well as Admiral Rogers, Director of NSA and Commander of U.S. Cyber Command.

Information Technology Sector Coordinating Council (IT-SCC): Palo Alto Networks is an Executive Committee member of the IT-Sector Coordinating Council, the principal entity for coordination between the Department of Homeland Security and IT sector companies and associations on a range of critical infrastructure protection and cybersecurity issues. The IT-SCC provides another official mechanism for Palo Alto Networks to collaborate with IT sector companies and DHS senior cyber officials on a range of sector-relevant policy, and cybersecurity issues.

Cyber Storm V: Palo Alto Networks was also actively engaged in the planning and execution of Cyber Storm V in early 2016. The biannual national cyber exercise is led by DHS and brings together over 1,100 U.S. government and private sector participants to test the cyber incident coordination processes that helped test and inform operational procedures and subsequent national policies. We commend DHS for their leadership and execution of these complex exercises, and would like to increasingly add realistic technical components to future iterations. Planning for Cyber Storm VI in 2018 has recently commenced, and we look forward to again working closely with DHS on this critical initiative.

Legislative Successes and Congressional Oversight of DHS Information Sharing Initiatives

As discussed in my introduction, this Committee has played a central role in passing a range of cybersecurity legislation that promotes responsible cyberthreat information sharing and strengthens DHS's statutory authority to execute its mission.

The information sharing portion of the Cyber Act (Title I) understandably garners most of the attention, and today's hearing demonstrates the need for oversight to ensure that Congress and DHS continue to identify areas of both progress necessary further improvements in its implementation.

In general, efforts to promote more direct engagement between DHS and the private sector technology community to address homeland security mission requirements should be encouraged. This can take the form of new legislation, such as Chairman Ratcliffe's recently introduced bill on leveraging emerging technologies, to oversight of existing laws, such as Title II of the Cybersecurity Information Sharing Act of 2015.

Thank you very much for the opportunity to testify before you today. I look forward to any questions you may have and your continued partnership on this critical issue.