Written Testimony of:

Major General (Ret.) John A. Davis, U.S. Army
Vice President, Public Sector
Palo Alto Networks

Before the:

Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Innovation
U.S. House of Representatives

Regarding:

"Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis"

May 5, 2021
2:30pm

Chairwoman Clarke, Ranking Member Garbarino, and distinguished members of the subcommittee, I am honored to appear before you today to discuss actionable policy solutions to address the unsustainable rise of ransomware. Thank you all for your leadership on this issue. I offer my commitment to work in partnership with you and your staff to support the subcommitte's oversight responsibilities on this issue.

That the Committee would hold this hearing shows that you see what we do: that ransomware is a profound and growing cybersecurity threat. Indeed, ransomware has crossed a strategic threshold. It is no longer purely a criminal nuisance driven by a profit motive. Rather, it is now impacting national security, economic stability and public health and safety of the national and international community on a massive scale.

Unfortunately, the problem is getting worse. An analysis by the Palo Alto Networks Unit 42 threat intelligence team concluded that the average ransom paid for organizations increased 171% year over year from 2019 ($115,123) to 2020 ($312,493). The highest-known paid ransom in 2020 doubled from the previous years ($5 million to $10 million). And adversary tactics are getting increasingly egregious. In 2020, for instance, ransomware disproportionately impacted the healthcare sector as hospital systems struggled to cope with the COVID-19 pandemic.

This unsustainable trajectory compelled Palo Alto Networks -- and the broader ecosystem of collaborators that comprised the Ransomware Task Force -- to take action. The Ransomware Task Force (RTF) is a public-private coalition of over 60 experts from government, industry, nonprofits and academia that came together to develop a comprehensive framework to tackle the ransomware threat. I am honored to represent the Task Force along with my colleague Megan Stifel at this hearing and discuss some of the key policy recommendations from the report the RTF released last week on April 29th.

The goal of the RTF was not simply to help the world better understand ransomware; we are well past that point. Nor was it to achieve an unrealistic outcome where all ransomware could be eliminated. Our objective was to proactively and relentlessly disrupt the ransomware business model through a series of coordinated actions which can be implemented by industry, government, and civil society. In total, the report identifies 48 actions across four strategic goals.

1. ***Deter*** ransomware attacks through a nationally and internationally coordinated, comprehensive strategy;
2. ***Disrupt*** the ransomware business model and decrease criminal profits;
3. Help organizations ***Prepare*** for ransomware attacks; and
4. ***Respond*** to ransomware attacks more effectively.

I will focus today on the report's recommendations that the United States should lead by example and execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign, coordinated by the White House, and that the United States should

develop a clear, actionable framework for ransomware mitigation, response and recovery, mapped to specific security capabilities organizations need to protect themselves.

Before turning to these points, I would like to introduce myself. As a reminder, I am here today in my capacity as a Co-Chair of the Ransomware Task Force. I am a retired U.S. Army Major General now serving as Vice President of Public Sector 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 in preventing successful cyber attacks and protecting our digital way of life. 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 across the U.S. Government to leverage technological innovation to solve critical cybersecurity challenges, including the threat of ransomware.

For those not familiar with Palo Alto Networks, we were founded in 2005 and have since become the world's largest cybersecurity company. We serve more than 80,000 enterprise and government organizations--protecting billions of people--in more than 150 countries. We support 95 of the Fortune 100 and more than 71% of the Global 2000 companies, and are partnered with elite technology leaders.

Palo Alto Networks collaborates extensively with key stakeholders across the U.S. Government and with like-minded countries internationally on both policy and operational matters. For example, Palo Alto Networks is a member of the President's National Security Telecommunications Advisory Committee (NSTAC), providing industry counsel on national security policy and technology issues for the White House and other senior U.S. government leaders; the Executive Committee of the Information Technology Sector Coordinating Council (IT-SCC), the principal entity for coordination between the Department of Homeland Security and IT sector; and the Defense Industrial Base Sector Coordinating Committee. Finally, we maintain robust threat intelligence sharing partnerships with DHS, the Intelligence Community and across the international community to share technical threat data and collaborate to support government and industry response to significant cyber incidents, like SolarWinds and Microsoft Exchange.

This commitment to meaningful collaboration with governments to tackle our shared cybersecurity goals is what compelled us to join the Ransomware Task Force. It has been an honor to be a part of this group and I have been humbled by the depth of passion and expertise this public-private partnership has brought to addressing this challenge. The diversity of thought, perspectives and experience that the RTF reflects should give you confidence in the viability and immediacy of the recommendations articulated in the reportat accomplishing these recommendations would lead to our overall shared strategic goals.

It's important to note that since its formation, the RTF has been deeply cognizant that we are not the first group to seek to tackle the ransomware issue. Many good initiatives have been stood up to focus on addressing cybersecurity and the threat of ransomware specifically. We stand on the shoulders of those efforts. The RTF never endeavored to replace that work- but instead consolidate and clarify the very best into a comprehensive strategic framework for action.

The RTF report recommendations are about dramatically reducing ransomware as a threat; there are no illusions about "solving ransomware." Instead, the report takes a practical approach to change the trajectory of this threat that has now crossed over a very dangerous threshold. We believe that our recommendations can reduce ransomware to a threat that can be more effectively managed like other threats that are dealt with through a practical risk management framework.

While I will highlight just a few of the report's key recommendations, I believe that the recommendations in the report should be viewed as a set of collective actions that should be applied with continuous, coordinated and overwhelming pressure. Some of these recommendations can immediately be pursued. Some will require creative policy solutions, including new legislation.

RTF Report Recommendation: **The United States should lead by example and execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign, coordinated by the White House.**

A foundational step is recognizing that the nature of the ransomware challenge will require a massive effort to sustainably shift the trajectory. While I am a retired Army General, I will borrow a phrase from my Naval comrades to say that our report calls for an "all hands on deck" approach. No single organization, public or private, has all of the capabilities, capacities, skills, experience, resources or authorities to act effectively in isolation.

It will take a team approach across government, industry, academia, nonprofits and the international community. This effort and our recommendations must be embraced at the highest levels of government and industry as a policy priority and given sufficient resources. To this end, we are heartened to see recent actions at the senior levels of the Department of Homeland Security and Department of Justice that signal the elevated prioritization of addressing this issue on a national and international level. But much more can and must be done to elevate this to even higher organizational levels within the Administration.

RTF Report Recommendation: **Develop a clear, actionable framework for ransomware mitigation, response and recovery.**

In addition to the need for greater strategic attention and coordination at the national policy levels, we also saw a core responsibility to help all organizations--states and localities, schools and critical infrastructure like hospital systems-- better prepare operationally for the threat of

ransomware attacks.

Within the RTF, I was a co-chair of the Prepare Working Group. Improving the ability to prepare for and even prevent most ransomware events from happening in the first place is the single most important function in reducing this threat to a manageable level. Building on best practices that have proven to be successful, clarifying and consolidating them, and making them easily accessible at appropriate levels is one of the most powerful tools we can employ. The adage "an ounce of prevention is worth a pound of cure" is especially true in the case of ransomware because, once you have been hit, you have already lost the battle and can only play catch up.

Most organizations, regardless of size or security acumen, are *aware* of the threat of ransomware. But most are not similarly empowered with adequate knowledge to quantify how finite resources can be applied to reduce their risk to ransomware threats specifically. We need to bridge the communications gap between IT and security professionals and senior organizational leadership. We need organizations to stop thinking about ransomware as a niche cybersecurity issue but instead as a core business continuity risk that must be managed in the same way as other physical disruptions.

The RTF saw the current state of awareness around ransomware as similar to the environment prior to 2014, when no authoritative compilation of best practices existed for cybersecurity generally. NIST responded by leading a multi-stakeholder process to create the *Framework for Improving Critical Infrastructure Cybersecurity.* In a similar way, the single most impactful measure we can take to help organizations is the creation of an internationally accepted framework that establishes clear actionable steps to prevent ransomware, and recover from it if prevention is not successful.

Of course, while technology isn't the only category associated with building this framework, it is certainly an important arrow in the quiver. Ransomware prevention technologies exist today and have demonstrated success. However, these technologies are not widely adopted. Coming from the cybersecurity industry, I have personally witnessed both traditional and emerging technologies that have demonstrated success in preventing ransomware attacks. Effective technologies include Endpoint or Extended Detection and Response (EDR/XDR) with automated behavioral analytics, fileless protections and deceptive technologies that stage objects as decoys or deploy decoy documents. These tactics employ automation and advanced analytics to flag modification to files and automatically prevent the ransomware encryption process. There are also cloud-based capabilities to launch unknown processes or applications in a container, which prevents malicious software or command and control channels from interacting with an organization's core network.

More traditional technologies at the network level include those that monitor and block common ransomware methods, such as Remote Desktop Protocol (RDP), phishing protections, capabilities that limit access to unknown or risky domains, and Secure Socket Layer (SSL) decryption to observe and scan content as it traverses the network. Finally, the traditional

capabilities such as Uniform Resource Locator (URL) filtering, Domain Name System (DNS) security, Intrusion Prevention Systems (IPS) and sandboxing capabilities provide protections against many common ransomware tactics, techniques and procedures.

Once the proposed ransomware framework's baseline security standards are established, it will be critical to map those standards to the specific security capabilities that organizations need to protect themselves. The creation of framework-aligned ransomware prevention reference architectures using industry leading technologies, consistent with the ongoing work at NIST's National Cybersecurity Center of Excellence, would be helpful towards this end.

Finally, these baseline best practices can also serve as a foundation for a number of potential policy actions to raise the bar of security across critical infrastructure and government. To this end, the RTF report suggests several incentives for entities that demonstrate a commitment to maturing their capabilities in alignment with the ransomware framework. For example, the report recommends the creation of a cybersecurity grant program for States and localities, where funding to procure ransomware-prevention focused security technologies could be unlocked through demonstrated alignment to the established best practice framework. Dedicated funding - aligned to strong cybersecurity planning and continuous vulnerability assessments - will enhance the resilience of state and local information systems, and provide a much-needed modernization of the security tools these governments use to prevent ransomware attacks. Opening up opportunities for multi-state grants will further drive innovation, security, and efficiency.

**

Chairwoman Clarke, Ranking Member Garbarino, 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.