Written Statement of

Grant Schneider

Senior Director of Cybersecurity Services, Venable LLP

to the

United States House of Representatives

Subcommittee on Cybersecurity, Information Technology, and Government Innovation, and

Subcommittee on Economic Growth, Energy Policy, and Regulatory Affairs

September 27, 2023

Chairwoman Mace, Chairman Fallon, Ranking Member Connolly, and Ranking Member Bush, members of the Committee, and your staff, thank you for the privilege to appear before you today.

I have spent my entire 30-year career focused on our nation's security. This includes over 20 years at the Defense Intelligence Agency, seven of which I served as the Chief Information Officer. I then spent six years at the Executive Office of the President, involved with all aspects of federal and critical infrastructure cybersecurity. I served as a Senior Director for Cybersecurity Policy on the National Security Council staff and most recently as the Federal Chief Information Security Officer, working with agencies to secure federal systems. For the past three years I have been a Senior Director of Cybersecurity Services at the law firm Venable, where I help our clients, both large and small companies from across all sectors, enhance their cybersecurity programs through the development and implementation of risk-management strategies. In addition, I assist our clients with the preparation, response, and recovery from various cyber incidents, including ransomware attacks.

Between my time in government and here at Venable, I have supported the investigation, response, and recovery of numerous cybersecurity and ransomware incidents. These experiences include:

- Leading the response and recovery for a regional healthcare delivery organization that was the victim of a ransomware event.
- Assisting clients who have been the victim of phishing attacks or social engineering schemes resulting in the re-direction of payments.
- Assisting clients who have been the victim of cyber extortion. This is where the malicious cyber actor threatens to disrupt a company's business or disclose sensitive information if a ransom is not paid.

- Creating playbooks and decision matrices to help clients consider the actions they may need to take in the event of a significant cybersecurity incident or ransomware attack.

- Responding to major cybersecurity incidents at federal agencies.

- Working with law enforcement, the Cybersecurity and Infrastructure Security Agency, the Intelligence Community, and other interagency partners on ways to disrupt malicious cyber actors.

I want to thank the committees for taking up the very important issues related to ransomware. Ransomware is a form of cyber-attack where the malicious actor typically steals sensitive information from the victim, encrypts the victims' files and systems, and demands a payment – the ransom – to return services to operation. Many of today's ransomware events are multiple extortion events where the threat actor also demands a payment in exchange for agreeing to not to sell or otherwise disclosure the stolen information. To be clear, ransomware is a means for malicious cyber actors to make money. It is rarely about foreign policy or espionage objectives like those we typically see from nation states. However, the policy discussions are complicated by the fact that many ransomware actors are protected and sometimes endorsed by the nations from which they operate.

Malicious cyber activity and ransomware have been around for decades; however, several factors have come together in recent years which have greatly expanded the frequency, scale, and public awareness of ransomware events. Nearly all organizations today, are dependent on technology to develop and deliver their service. This includes everything from school districts, to hospitals, to financial services, to energy, to transportation, and every other critical infrastructure sector. These digital enhancements provide increased productivity, convenience, and broad delivery of services to customers. At the same time, more critical services and sensitive data have moved to an internet accessible environment. Correspondingly, ransomware actors have

increased access to technical capabilities, anonymous payment systems, and safe havens from which to operate.

U.S. Government organizations have taken steps to help protect private organizations and individuals from ransomware. The Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, and the Federal Trade Commission have published alerts and guides to help educate private organizations on steps they can take to help defend against ransomware attacks. These include recommending the implementation of defensive cybersecurity controls that every organization should implement such as:

- Phishing resistant multi-factor authentication.
- A robust set of system backup and recovery tools and procedures.
- Timely patching of hardware and software systems with the most recent security updates.
- Encryption of data at rest and in transit.
- Training for employees to be able to recognize phishing e-mails and to recognize social engineering attempts.

In recent years, the Department of Justice has stepped up counter ransomware activities to include dismantling the Hive ransomware group. The Hive group was responsible for extorting and attempting to extort hundreds of millions of dollars of ransoms from organizations within the US and around the world. Hive used a ransomware as a service model where they sold their capabilities to other malicious actors thereby increase the number of victims they can attack.

While governments around the world should work together in a coordinated fashion to disrupt and combat ransomware, policy makers need to consider steps to change the value proposition for ransomware actors.

In our policy discussions we cannot lose sight of the fact that ransomware can have devastating operational, economic, and reputational impacts on victim organizations. During a ransomware event, government organizations, including law enforcement, can provide a limited amount of support. Victims of ransomware are often left with an unsavory set of options. In many cases the victim organization must choose between restoring services quickly by paying the ransom or working to reconstitute their systems and restore operations on their own. Reconstituting an organization's systems is a costly and time-consuming process during which service delivery may be impaired and result in the loss of significant revenue. Often, paying a ransom can be the most time and cost-efficient approach to getting systems running and restoring data.

Given these dynamics for victims, ransomware remains a pernicious and prevalent threat to large and small businesses, public sector entities, and critical infrastructure organizations. In short, it's bad. That said, there is hope. The U.S. – through the Department of Justice – has invested heavily in disrupting ransomware activities across the globe. Cybersecurity luminaries have partnered with policy professionals to propose legal and policy updates that will empower law enforcement officials and other cyber defenders to pursue these bad actors and build resilience across our digital ecosystem. We will continue to develop these ideas while working with companies and public sector entities to harden their networks and protect their data.

Thank you again for the opportunity to speak with you today, and I look forward to your questions.