Written Statement

Tom Kellermann

Head of Cybersecurity Strategy

VMware, Inc.

Before the U.S. House of Representatives National Security, International Development and Monetary Policy Subcommittee

May 28th, 2020

Chairman Cleaver, Ranking Member Hill, Members of the Subcommittee, I am Tom Kellermann, Head of Cybersecurity Strategy for VMware Inc. I have 22 years of experience in cybersecurity. VMware is the fifth largest software company in the world. We have revenues of over $10 billion and more than 31,000 employees. We are headquartered in Silicon Valley, California, with 125 offices throughout the world, serving more than 75,000 partners and 500,000 customers, including 100 percent of the Fortune 500. Our software is present in 88% of the world data centers and was the enabler for data center consolidation worldwide, savings organizations billions in hardware costs. Thank you for the opportunity to brief the Subcommittee today.

The financial sector has long been a major target of the world's cyber criminals. VMware's Carbon Black has conducted several in depth analysis over the years, detailing the trends, threats and recommendations to protect the industry. I have sent to the Subcommittee our latest report which highlights how financially motivated criminals have evolved from stagecoaches and stickups to targeted cyberattacks. Over the past five months, cyber defenders have seen

a high level of innovation from cybercriminals, who are leveraging new tactics, techniques and procedures (TTPs) to maintain persistence and counter incident response efforts.

At an alarming rate, transnational organized crime groups are leveraging specialist providers of cybercrime tools and services to conduct a wide range of crimes against financial institutions, including ransomware campaigns, distributed denial of service (DDoS) attacks, business email compromise (BEC) scams and access mining. Criminals are increasingly sharing resources and information and reinvesting their illicit profits into the development of new, even more destructive capabilities. The growing availability of ready-made malware is creating opportunities for even inexperienced criminal actors to launch their own operations. When combined with a steady commercial growth of mobile devices, cloud-based data storage and services, and digital payment systems, cybercriminals today have an ever-expanding host of attack vectors to exploit. Every organization—providers of financial services, in particular—must remain vigilant in the face of these evolving threats. From February to April 2020, amid the COVID-19 surge, cyberattacks against the financial sector increased by 238 percent, according to VMware Carbon Black data. Cybercriminals are taking advantage of COVID-19, and they are doing so in tandem with the news cycle.

The Bank Heist has escalated to a hostage situation. According to the Modern Bank Heists Report which is attached, 80 percent of surveyed banks said they've seen an increase in cyberattacks over the past 12 months, marking a 13 percent increase over 2019. And 2020 has offered a glimpse into a new world. 25% of surveyed financial institutions said they were targeted by destructive attacks over the past year. Destructive attacks are rarely conducted for

financial gain. Rather, these attacks are launched to be punitive by destroying data. 33 percent of surveyed financial institutions said they've encountered island hopping, an attack where supply chains and partners are commandeered to target the primary financial institution.

Cybercriminals are evolving in both attack sophistication and organization. The financial sector is the most secure industry in the world, but it is also being targeted by cybercriminals and nation-states. We, must pay close attention to how we respond to these threat actors and what their ultimate goal is—hijacking your digital transformation efforts via island hopping. Trust and confidence in the safety and soundness in the US financial sector is dependent on cybersecurity.

There are four opportunities for strategic public policy:

1. Tax credits for cybersecurity investment.
2. Shared service providers to the financial sector must be held to comply with the FFIEC Information Security Handbook as they are being targeted for island hopping which can create systemic risk.
3. The United States Secret Service should be migrated back into Treasury and their budget should be increased.
4. Anti-money laundering and forfeiture regulations must be modernized to seize the virtual currencies and alternative payments which are used in the cybercrime conspiracies. These seized funds should be explicitly allocated to cybersecurity investment across US critical infrastructures.

Chairman Cleaver, Ranking Member Hill, thank you for the opportunity to participate in this important roundtable. I am happy to answer any questions the Subcommittee might have.