Opening Statement of Ranking Member Morgan Griffith
Subcommittee on Oversight & Investigations Hybrid Hearing
"Stopping Digital Thieves: The Growing Threat of Ransomware"
July 20, 2021
As Prepared for Delivery

Thank you, Chair DeGette, for holding this hearing, especially considering the recent increase in ransomware attacks across our nation, including high-profile attacks such as Kaseya, Colonial Pipeline, and SolarWinds. I also want to thank the witnesses for taking the time to join us today.

Cybersecurity is integral to all organizations and should be treated as a priority for maintaining the health and security of an organization, as well as any other individuals or entities that are affiliated with that organization. The need for more rigorous cybersecurity protections exists across all industries, including health care, oil, gas, water, and electricity. Any network with vulnerabilities can be subject to a cyber threat, and the frequency of cyberattacks is increasing exponentially.

The reach of the most recent cyberattacks demonstrates how serious this issue is. For example, the Colonial Pipeline, one of the most critical pieces of energy infrastructure, was the target of a ransomware attack in May. The attack halted all pipeline operations and caused supply disruption up and down the East Coast for over a week – which led to higher gas prices and longer lines. More recently, over the Fourth of July holiday, the Kaseya supply chain ransomware hack affected medium and small-sized business globally. Both of these attacks appear to be Russia-linked, which is the most recent showing of the cyber threat Russia poses to the U.S.

Although the recent attacks appear to be linked to Russia, adversaries of cyber-attacks originate in different foreign nations, vary in the size of the criminal enterprises, and their approaches to gaining access to systems range in their level of sophistication. However, no one industry or part of our nation's critical infrastructure is immune to the threats posed by these malicious actors. Cyberattacks have the potential to cause real harm, depending on the severity and target.

In health care in particular, direct harm is almost a certainty. Anytime information in the health care and public health sector is compromised, it poses a risk to providers, patients, and all those who serve and supply them. But it is not just data and privacy that are compromised – ransomware attacks can have a significant impact on patient health.

For example, in May, a ransomware attack hit a San-Diego based health system, Scripps Health, and the cybercriminals stole data on close to 150,000 patients. This forced the Scripps Health system to not be fully up and running until a *month* after the ransomware attack. These types of incidents are detrimental to the care available to the community and put a major strain on the surrounding health care system in the region. As the ransomware recovery timeframes increase from days to months, the amount of damage skyrockets. In a hospital's case, that can mean a difference between life and death.

The recent ransomware attacks are providing lessons about the importance of cybersecurity. These systems are fragile. Although it is impossible for a system to be completely resilient against any cyberattack, there is much more the federal government, cybersecurity organizations, cyber victim organizations, and the private sector can do to detect, respond, and recover from ransomware threats. This is a shared responsibility and we need everyone to do their part.

The United States has great cyber experts found in both the federal government and the private sector that supply the key building blocks to revamping our nation's cybersecurity. The federal government has strong resources to prevent attacks, respond to attacks, and hold criminals accountable. We just need to see more of it—and we need to make better use of these resources.

Coupled with the federal government resources, we have private sector firms that offer cybersecurity consulting for a range of organizations at different entry points in their cybersecurity cycles and at different levels of cybersecurity risk. Moreover, we have experts that focus exclusively on industrial control systems

(ICS) and operations technology (OT) cybersecurity. We also have non-profit networks that design solutions for emerging threats and private companies with specialized professionals to disrupt criminal enterprises. We need to ensure an open line of communication, coordination, and information sharing in the cyberworld and delineate proper responsibilities for developing cybersecurity strategies to the appropriate entities.

It is impossible to eliminate all cyber threats to our nation. However, we need to do more to better prevent and detect ransomware attacks so that we can thwart worst-case outcomes, especially when it comes to critical infrastructure. I look forward to hearing from the witnesses here today given their expertise and experiences in this space and am eager to learn more about what we can do to help prevent and detect future ransomware attacks. I yield back.