OPENING STATEMENT
RANKING MEMBER ROB PORTMAN
RISING THREATS: RANSOMWARE ATTACKS AND RANSOM PAYMENTS ENABLED BY CRYPTOCURRENCY

June 7, 2022

Thank you, Mr. Chairman. And thank you to our witnesses for joining us.

Today we will hear from a private sector panel of cybersecurity professionals and incident responders who will provide their unique perspective on what can be done to combat ransomware.

The frequency and severity of ransomware attacks continues to grow. Ransomware groups have professionalized their operations using a business model often called ransomware-as-a-service—which involves ransomware developers selling or delivering their malware to individuals called "affiliates" who actually carry out the attack. This allows ransomware gangs to conduct more attacks with broader impact.

Back in March, I released a report documenting the experiences of three American companies victimized by one of the most notorious Russian ransomware gangs, called REvil [are-evil]. The companies profiled in the report are from different business sectors and vary significantly in size, revenue, and IT resources. Despite those differences, they all fell victim to REvil. This underscores the broad threat ransomware presents and the proactive steps all organizations must take to implement cyber best practices.

REvil was largely believed to be offline following the arrests of several key members last fall. But public reports indicate the gang may be resuming operations. We know it is common for ransomware criminals to claim retirement only to "rebrand" and reemerge under a new name.

About a year ago, this Committee held a hearing on the Colonial Pipeline ransomware attack. That incident was a painful reminder that these attacks have real-world consequences impacting the everyday lives of Americans.

Attacks like Colonial Pipeline or any of the numerous significant ransomware attacks over the past year demonstrate how difficult it is for organizations to account for all vulnerabilities and defend against sophisticated cyber adversaries.

Recognition of this challenge is one of the reasons Chairman Peters and I drafted cyber incident reporting legislation which I am proud to say became law in March.

This law will enhance our nation's visibility into cyberattacks against the United States and enable a more effective response including warning potential victims. It is important that CISA works with industry experts and stakeholders to implement this law quickly.

We know ransomware attacks will continue to be a national security threat for the foreseeable future. As the committee of jurisdiction over cybersecurity, we will continue to work to identify solutions that address the threats associated with ransomware attacks and the ways we can fortify our defenses.

I look forward to the testimony of our witnesses on these important issues.