Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: **Rising Threats: Ransomware Attacks and Ransom Payments Enabled by Cryptocurrency**
June 7, 2022

Thank you to our witnesses for joining us. Today's hearing will provide an important opportunity to discuss the rising threat posed by ransomware attacks, and the role cryptocurrencies play in enabling these harmful cybercrimes.

In recent years, we have seen a scourge of increasingly complex and sophisticated ransomware attacks on both public and private networks, where the attackers prevent access to an entity's computer systems or threaten to release stolen data unless a ransom is paid.

From the Kaseya ransomware attack that affected between 800 and 1,500 small businesses, to alarming attacks on our critical infrastructure that caused gas shortages across the East Coast and temporarily shut down processing plants for the world's largest meat supplier, ransomware attacks have caused significant disruptions to daily life and imposed serious economic costs.

A single ransomware attack can force businesses to close their doors permanently, even if they pay the ransom demand. Cybercriminals may shut down computer systems, expose sensitive data, or erase data entirely, causing significant disruption to business continuity. Some of the longer-term impacts may include lost revenues, reduced profits, damage to brand reputation, employee layoffs, and loss of customers.

These malign actors almost exclusively demand cryptocurrencies when extorting large sums of money, because they can take steps to obscure their transactions and circumvent regulatory scrutiny, making payments more difficult to trace.

In 2020, according to a Chainalysis study, malicious hackers received at least $692 million in cryptocurrency extorted as part of ransomware attacks, up from $152 million in 2019, and over a 300 percent increase year-over-year. These figures are likely a drastic underestimation of the actual number of attacks and ransom payments made by victims.

While Bitcoin and many other cryptocurrencies provide a public ledger of transactions, known as a "blockchain," cryptocurrency wallets are not tied to an individual person, meaning account holders can take steps to conceal their identity to avoid being held accountable for criminal activities.

Anti-money laundering and other banking regulations that are meant to prevent criminal use of currency, including cryptocurrency, are also often inconsistently enforced, particularly in foreign jurisdictions, where many attackers are based.

For example, last year, according to Chainalysis, approximately 74 percent of global ransomware revenue went to entities either likely located in Russia, or controlled by the Russian government. And attacks from Russia-based entities are only expected to increase, especially as the United States continues its support of Ukraine against Russia's illegal invasion.

Last month, I released a report examining the role cryptocurrencies play in incentivizing and enabling ransomware attacks, and the resulting harm these attacks have on victims.

I now move to introduce this report as part of the hearing record. … Without objection, the report will be entered into the record.

My investigation found that the federal government lacks sufficient data and information on ransomware attacks and the use of cryptocurrency as ransom payment in these attacks, and must collect better data to understand the scope of the threat.

The cyber incident reporting law that Ranking Member Portman and I authored and passed earlier this year marks a significant first step to getting the information the government needs to combat this growing threat.

The legislation will require critical infrastructure owners and operators to report cyber-attacks within 72 hours and ransomware payments within 24 hours, and I look forward to working with the Administration to ensure it is swiftly and effectively implemented.

The more information we have, the better suited we will be to combat ransomware attacks. That means continuing to build off our bipartisan cyber incident reporting legislation by holding foreign adversaries and cybercriminals accountable, and finding ways to reduce the incentives to conduct these attacks in the first place, including by examining their use of cryptocurrency.

While I am grateful to the many federal law enforcement and regulatory agencies that have taken steps to address cybercriminals and the rising threat of ransomware attacks, more must be done to ensure cryptocurrencies are monitored appropriately, like their non-digital counterparts.

Finally, in addition to addressing ransomware attacks and use of cryptocurrency as ransom payment in those attacks, Congress must examine other criminal activity involving cryptocurrency that threatens our nation's economic and national security, such as human trafficking, the flow of illicit drugs across our borders, and other serious crimes.

I look forward to hearing from today's panel of expert witnesses who can further elaborate on the uses of cryptocurrency in ransomware attacks, and provide answers to ensure we have the necessary tools and resources to tackle this issue head on.