COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Chairman Bennie G. Thompson (D-MS)

Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure

June 9, 2021

Last month, malicious hackers infiltrated Colonial Pipeline's network and infected its IT systems with ransomware. For nearly a week, 5,500 miles of pipeline supplying 45 percent of the fuel on the East Coast were shut down, and panic buying resulted in fuel shortages in the southeast. Since pipeline service was restored, we have learned more about what happened.

We know hackers exploited an unprotected VPN account that was no longer in use to gain access to Colonial Pipeline's networks. We know Colonial Pipeline paid the ransom demand – and the FBI has since recovered most of it. And we know Colonial Pipeline is hardly alone – this spring, ransomware attacks hit the world's largest meat processor, transportation systems in New York City and Martha's Vineyard, and Scripps Health in San Diego.

But the potential impact of a long-term shut down of the country's biggest pipeline crystalized the devastating consequences of ransomware. More importantly, it raised serious questions about the cybersecurity practices of critical infrastructure owners and operators and whether voluntary cybersecurity standards are sufficient to defend ourselves against today's cyber threats.

I was glad to see the Transportation Security Administration issue a security directive to mandate some security requirements for the pipeline industry—but more requirements may still be needed. To drive the policies necessary to defend against and mitigate the impacts of future ransomware attacks, we need a complete understanding of the circumstances surrounding the ransomware attack against Colonial and the decisions it made during incident response.

Today, our goal is to examine the cybersecurity practices in place at Colonial prior to the May 2021 ransomware attack, and assess whether other critical infrastructure operators might be similarly situated and vulnerable. We need to understand the degree to which Colonial utilized the full range of security resources made available by TSA – Colonial's sector risk management agency – and the Cybersecurity and Infrastructure Security Agency (CISA). I am troubled by reports that Colonial declined repeated offers by TSA over the past year to assess its security defenses. We also need to understand whether Colonial had a ransomware incident response and continuity of operations plan and whether it had been practiced and tested.

Government officials and cybersecurity experts have been warning about the growing threat of ransomware for years. We need to know how private sector entities like Colonial acted on those warnings. Finally, we need to understand the threat actor – how it targets victims, what tools it utilizes to infiltrate networks, and how we can deter this kind of behavior.

Before I close, I would like to commend the FBI for its work recovering Colonial's ransomware payment and depriving the hackers of the financial benefit of their malicious cyber activity. I hope the FBI's success serves as an incentive for future ransomware victims to engage with law enforcement early. And, I hope Colonial will use the recouped money to make necessary improvements to its cybersecurity.

# # #

Media contact: Adam Comis at (202) 225-9978