Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack
June 8, 2021

Mr. Blount, welcome to the Committee. Thank you for joining us for this important discussion on the harmful cyber-attack against your company, Colonial Pipeline, and how we can work to strengthen coordination and response to these serious cybersecurity incidents.

When Colonial Pipeline was forced to shut down operations last month due to a ransomware attack, millions of Americans up and down the East Coast had their lives disrupted by gas shortages and price increases.

In the weeks since your company was struck, we have seen a series of other attacks, on everything from our transportation networks to meat-packing centers. Those private sector strikes follow especially damaging attacks on our government, including the extensive SolarWinds hack last year.

While the objectives of these attacks differ, they all demonstrate that bad actors, whether criminal organizations or foreign governments, are always looking to exploit the weakest link, infiltrate networks, steal information, and disrupt American life.

Mr. Blount, I am glad your company continues to recover from this malicious attack and that the FBI was able to recover millions of dollars in ransom paid. But I am alarmed that this breach ever occurred, and that communities from Texas to New York suffered as a result.

I appreciate that you have joined us today, to provide answers to the Committee and the American people on how a group of criminals was able to infiltrate your networks – steal nearly 100 gigabytes of data in just two hours – and then lock your systems with ransomware to demand payment. I am also looking forward to hearing an update on your progress to recover from this serious breach.

Private entities, especially those that are critical to our nation’s infrastructure, are responsible for assessing their individual risk and investing in the technology to prevent breaches and ensure they can continue providing service to customers who rely on them for basic necessities, like fuel.

At the same time, the federal government must develop a comprehensive, all of government approach to not only defend against cyber-attacks, but punish foreign adversaries who continue to perpetuate them or harbor criminal organizations that target American systems.

This approach requires bolstering our defenses, and using the full might of our diplomatic, military, and intelligence capabilities.

We must also ensure private entities, like Colonial, are providing the federal government with timely and relevant information in the event of major incidents.

We need federal agencies charged with cybersecurity – like the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency – to understand the extent of these attacks and how best to support victims.

Make no mistake – if we do not step up our cybersecurity readiness – the consequences will be severe. The ransomware attack on Colonial Pipeline affected millions of Americans. The next time an incident like this happens – it could be even worse.

As Chairman of this Committee – I am committed to prioritizing policies that will help secure our critical infrastructure networks – including in the proposed infrastructure package Congress is negotiating.

Protecting the American people from these sophisticated – harmful – and growing attacks will not be easy. We must learn from our past mistakes – find out what went wrong – and work together to tackle this enormous challenge. Inaction, however, is NOT an option.