COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

## Joint Hearing Statement of Transportation & Maritime Security Subcommittee Chairwoman Bonnie Watson Coleman (D-NJ)

## *Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack*

**June 15, 2021**

The impacts of the May 7th ransomware attack on Colonial Pipeline were far-reaching. As we all know now, nearly half of the East Coast's fuel is supplied by the Colonial Pipeline. When the pipeline was shut down, Americans struggled to fill up their gas tanks, and the incident threatened to cause major disruptions to the economy and well-being of our country. That's why it's so important for us to have a conversation today about the Federal government's response to the Colonial incident and its role in ensuring the cybersecurity of our critical infrastructure.

Last week, we heard from the CEO of Colonial Pipeline about how his company responded to the ransomware attack against it. I also asked him why his company, prior to the attack, appears to have resisted TSA's efforts to assess the pipeline's security prior to the attack. Today, we will hear from TSA and CISA – the DHS components charged with ensuring the cybersecurity of our nation's pipelines and responding to cyber incidents.  I am looking forward to learning not only about TSA and CISA's engagement with Colonial before and after this incident, but also about their plans to ensure we are better prepared next time. And unfortunately, we know there will be a next time.

In recent weeks, we've seen two transportation systems fall victim to ransomware attacks in New York City and Massachusetts. Hospitals have been brought to a halt. Even one of our nation's largest meatpackers was shut down. We must ask ourselves: what's next? Our power grid? Our aviation system? Maybe next time it won't be foreign hackers looking for a quick pay day, but rather a nation-state looking to cripple our economy. Given the magnitude of these threats, we need to ensure CISA and sector-specific agencies like TSA have the tools and authorities they need to take action – and that they use them.

In the pipeline context, since TSA's establishment nearly twenty years ago, it has been the principal Federal entity responsible for pipeline security. To this end, TSA publishes pipeline security guidance and conducts pipeline security assessments and inspections – including assessments that focus specifically on cybersecurity.  To date, these assessments have been voluntary—and unfortunately, voluntary standards have proven insufficient.

According to TSA, prior to the attack TSA asked Colonial Pipeline on no less than thirteen occasions to participate in physical and cyber pipeline security assessments. Citing COVID-19, Colonial repeatedly delayed and chose not to participate. On multiple occasions, Colonial didn't even bother responding to TSA's emails. In fact, Colonial still has not agreed to participate in the physical assessment, and only agreed to cooperate with TSA's cybersecurity assessment three weeks after the ransomware attack occurred. What's more, when a Member of this Committee asked Colonial's CEO whether he'd accept CISA's assistance, he politely but firmly declined. If this is at all indicative of how pipeline owners and operators view their regulators, we have a problem.

Although many of these systems may be owned by private companies, when you operate infrastructure that we all depend on, you have a responsibility to the public. The good news is that the TSA Administrator has existing statutory authority to address this. Just a few weeks ago, TSA used this authority to impose the first mandatory cybersecurity requirements on pipeline owners and operators. Specifically, now they must report breaches, designate cybersecurity coordinators, and self-assess their compliance with TSA's security guidance. This is an important first step, but there is clearly more that needs to be done.

We must resource and empower TSA and CISA to act boldly and swiftly to ensure operators of pipelines and all other forms of transportation harden their systems. Meanwhile, it is similarly important that other agencies in the Federal government respect TSA and CISA's experience and expertise on these matters. The cybersecurity of our critical infrastructure is too serious for us to reinvent the wheel by providing duplicative authorities to the Department of Energy. DHS has the existing statutory authority and technical talent we need to tackle this challenge.

Finally, before I conclude, I must note my disappointment that the FBI declined an invitation to attend this hearing. It is critical that Members fully understand the FBI's role and efforts in countering cyber threats, and I look forward to their participation in future events on these topics.

# # #

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