COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

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

June 15, 2021

The attack on May 7 that resulted in the week-long shutdown of 5,500 miles of petroleum pipeline on the East Coast clearly represents a significant cyber-attack on critical transportation infrastructure. It is clear that the future will bring more attacks like this, whether from organizations like DarkSide that seek to exploit cybersecurity weaknesses for profit or foreign enemies seeking to weaken our nation.

The Federal government must be prepared to fight off attacks and respond to successful security breaches swiftly and effectively. The Cybersecurity and Infrastructure Security Agency is the lead federal coordinator for securing critical infrastructure from cyber-attacks, and the Transportation Security Administration is the designated sector risk management agency for pipelines. Yet Colonial failed to properly engage with TSA in recent months in order to safeguard their pipelines against attack and repeatedly rejected technical assistance from CISA following the ransomware incident.

While I am pleased that Colonial has finally agreed to a virtual cyber-security assessment from TSA, I am alarmed that they refused to do so until three weeks after an attack that resulted in the full shutdown of their pipeline. Despite the authority placed within the Department of Homeland Security to respond to cyber attacks on pipelines, including through TSA's authorities to issue emergency security directives, the Department of Energy was made the lead agency for response to the Colonial incident. Additionally, the Federal government did not deem the attack a "significant cyber incident" as defined by policy, despite its substantial impact.

Cyber incident response plans have been carefully crafted to ensure proper government response to incidents, and we must ensure they are followed appropriately. The attacks on Colonial and others provide opportunities to learn improve the resiliency of the pipeline sector and critical infrastructure across the United States. I was pleased to see TSA take initial action by issuing the first ever mandatory cybersecurity requirements for pipelines. These new requirements went into effect on May 28 and will be critical in improving coordination among the pipeline industry, CISA, and TSA.

More must be done to increase protections for our pipelines and allow federal authorities greater ability to assess weaknesses in critical transportation infrastructure. Unfortunately, cyber criminals are not going anywhere anytime soon. In fact, they are getting smarter, and cyber-attacks are likely to become more common. We must ensure the Department of Homeland Security remains at the forefront of protecting our critical infrastructure from these threats.

# # #

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