COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Markup of H.R. 2795, H.R. 2980, H.R. 3138, H.R. 3223, H.R. 3243, H.R. 3263, & H.R. 3264

May 18, 2021

Just over ten days ago, a ransomware attack against one of the nation's largest pipeline companies has brought a new urgency to our work. The Colonial Pipeline ransomware attack caused 5,500 miles of pipeline along the East Coast to shut down for days, triggered fuel shortages across the northeast.

This attack follows a string of disturbing cyberattacks against government entities and the private sector – from SolarWinds and Pulse Connect Secure to Microsoft Exchange Server and the Oldsmar Water facility. Since the beginning of this Congress, this Committee has engaged in extensive oversight of these events and how the Federal government partners with others to defend our networks. Today, we are considering measures resulting from that oversight.

There is the "State and Local Cybersecurity Improvement Act, " as authored by the Chairwoman of our Cyber subcommittee, Ms. Clarke, that seeks to authorize a new $500 million grant program to provide State and local governments with dedicated funding to secure their networks from ransomware and other cyber attacks.

We also have the "Cybersecurity Vulnerability Remediation Act," as introduced by Ms. Jackson Lee, that authorizes the development and distribution of cyber "playbooks" to critical infrastructure owners and operators to provide them with mitigation strategies against the most critical, known vulnerabilities – especially those affecting software or hardware that is no longer supported by a vendor, including for industrial control systems.

We are also considering the "CISA Cyber Exercise Act," a bill that Ms. Slotkin introduced that seeks to establish a National Cyber Exercise program within CISA to promote more regular testing and systemic assessments of preparedness and resilience to cyber attacks against critical infrastructure.

Finally, we will be taking up the "Pipeline Security Act," as authored by Mr. Cleaver, which seeks to enhance the Transportation Security Administration's ability to guard pipeline systems against cyberattacks, terrorist attacks, and other threats. As the principal Federal agency responsible for protecting pipelines, TSA is fortunate to have CISA as its sister agency within DHS to support its pipeline security mission. Importantly, this legislation codifies collaboration between TSA and CISA to bolster the security of this critical infrastructure.

In addition to these four cybersecurity measures, there are three measures introduced by Committee Republicans that have my support.

# # #

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