COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis

May 5, 2021

Last fall, in my district, the Yazoo County School District paid $300,000 to a cybersecurity firm to recover data that was encrypted in a ransomware attack. For a county of fewer than 30,000 people, that is a lot of money. In fact, that is 1.5% of the school district's annual budget that had to be spent on just one incident. Unfortunately, Yazoo County is not alone. School districts across the country have been forced to respond to ransomware attacks in the midst of the unprecedented challenges they have faced during this pandemic, where access to technology has been more important than ever. To be clear, this is a national security issue.

We cannot expect school districts like Yazoo County to defend themselves alone when these attacks are coming from sophisticated criminal gangs based overseas that frequently have the tacit or even direct support of adversaries like Russia or North Korea. And the harms these communities face are frequently not just financial. Ransomware attacks have led to cancelled school days, delayed medical procedures, and disruptions to emergency response services. For these reasons, it is essential that we pass Chairwoman Clarke's State and Local Cybersecurity Improvement Act to ensure state, local, territorial, and Tribal governments get the assistance they need to defend their networks.

I am proud to be a cosponsor of this important legislation and look forward to working with Chairwoman Clarke and the bill's bipartisan group of supporters to get it enacted into law. We cannot afford to wait any longer to provide the funding necessary to protect our state and local governments.
Fortunately, it is clear that the Biden Administration has made addressing ransomware a priority.

From Secretary Mayorkas announcing DHS's 60-day sprint on ransomware to the Justice Department's new task force, the executive branch is now demonstrating the coordinated approach that reflects the gravity of this threat. This Committee stands ready to work with them to ensure the resources and authorities are there to fulfill this critical mission. The recently released Ransomware Task Force report provides numerous recommendations on how we can develop a cohesive approach to combatting ransomware.

I appreciate the hard work of the members of the Task Force in putting together this comprehensive document in just the last three months, reflecting the urgency of this growing crisis. The report makes clear that despite the many challenges presented by cryptocurrencies and foreign adversaries that help disguise and protect ransomware criminals, there are important steps the government can take to enhance defenses, improve information sharing, and collaborate with partners in the private sector and internationally to tack this problem. These proposals have given Congress much to consider, and we are committed to ensuring that this issue remain a priority for Congress, so we can take meaningful action.

I am eager to hear more from the witnesses on these recommendations and how they envision DHS's role in implementing them.

# # #

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