COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Cybersecurity Challenges for State and Local Governments: Assessing How the Federal Government Can Help

June 25, 2019

Just last week, Riviera Beach - a small city in Florida - agreed to pay a $600,000 ransom demand after hackers crippled city computer systems. Unfortunately, Riviera Beach is hardly alone. Hackers have been wreaking havoc on cities from Atlanta to Baltimore to Albany. These bad actors range from unaffiliated cyber criminals to sophisticated state actors–including Iran–and their interest in breaching state and local networks is only growing. Since the Russian government engaged in a historic campaign to meddling in the 2016 elections, officials at all levels of government have devoted time and resources to improve the security of election infrastructure. For its part, Congress appropriated $380 million–a down payment–to fund grants to State and local election officials to replace unsecure election equipment, improve network security, and provide cybersecurity training to election officials.

Additionally, for two fiscal years, Congress has provided the Cybersecurity and Infrastructure Security Agency additional funding to provide cybersecurity services - upon request - to election officials. But administering elections is only one of the many important responsibilities carried out by State and local governments. So far this year, there have been over 20 reported cyber attacks against government agencies. These attacks disrupted networks in local police departments, offices that process real estate transactions, and public health departments, just to name a few. The impacts ranged from jeopardizing 9-1-1 calls, grinding real estate transactions to a halt, and preventing health officials from warning the public when a bad batch of illegal drugs causes overdoses. Unfortunately, the sophistication of hackers is outpacing the speed at which state and local governments can implement IT modernization programs and phase out legacy technologies. Moreover, the attack surface is growing as more jurisdictions are integrating 'smart city' technologies into the execution and delivery of government services.

As other sectors improve their cybersecurity posture, state and local governments struggling to keep pace with technology are becoming low-cost, high-value targets. It is time for the Federal government to do more. Every year, States assess cybersecurity as one of the 32 core capabilities in which they are least proficient. At the same time, States rarely use their Homeland Security Grant to invest in cybersecurity as they stretch these funds to support traditional terrorism preparedness and response capabilities.

Make no mistake, State and local governments need to invest in security, especially as they invest in smart city technology. But it is time to improve the way the Federal government helps them. Toward that end, I am pleased that Mayor Keisha Lance Bottoms is here today to share the lessons learned from the ransomware attack in Atlanta and to understand how the Federal government can better help victims prevent, respond to, and recover from cyber attacks. I am also eager to hear from the MS-ISAC, which serves as the cyber threat information sharing hub for State and local governments, and spearheads state and local coordination on securing election infrastructure. Finally, I look forward to understanding the disparate impacts of cybersecurity incidents on vulnerable populations and how the Federal government can partner with state and local governments to address them. Addressing the cybersecurity challenges ahead will require strong partnerships among all levels of government, and I am eager to understand how Congress can help ensure that Federal resources are most effectively leveraged.

# # #

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