COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity, Infrastructure Protection, and Innovation Subcommittee Chairman Cedric Richmond (D-LA)

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

June 25, 2019

This is a topic that I believe deserves far more attention than it gets. Since joining this Subcommittee, I have found that–while we can all agree that cybersecurity is an important topic–it can start to feel unapproachable to people on the ground. As Chairman, I want to spend some time looking at how cybersecurity impacts real people–like the ones I represent in the 2nd District of Louisiana. I know that my constituents work long hours and have hard jobs, sometimes more than one. Many of them are not thinking about phishing emails or ransomware or whether a hostile foreign government has gained access to the networks that control their drinking water, transportation, or medical care. And, while the Federal government has an important role to play in securing these networks, state and local governments own them. The staffing, structure, and resources available to state and local agencies vary across the country–but many of them are operating with a shoestring budget. And, like Federal agencies, they are increasingly being targeted with sophisticated cyberattacks.

Time and again, we've seen that these attacks can be debilitating–taking out the tools and services people need to access health benefits, buy a home, or even call 9-1-1. As any city official who has recovered from one of these cyber disruptions can tell you, the aftermath can have a hefty price tag. This is a drain on taxpayer dollars, time, and labor–all of which are in short supply at the state and local levels. We also know that these attacks are becoming more frequent and more advanced. According to security firm Recorded Future, there have been at least 170 ransomware attacks carried out on county, city or state governments since 2013–including over 20 reported so far this year. That's just the incidents that were reported. The actual numbers are probably far higher.

But there's another problem, as well. Today, we rely on the internet to an extent that we never have before. Access to connected devices–and an understanding of how to use them securely–is the very foundation for economic mobility. Yet we also know that many in our communities do not have the same means, access, or opportunity to build a level of comfort with technology. While we talk a lot about how automation might impact the workforce, we talk less about how poor cyber hygiene and low tech literacy can present a real economic barrier to entry. Right now, studies show that the most vulnerable, under-served among us–low-income, immigrants, or elderly populations–are the most likely to fall victim to an online scam or click on the wrong link. These mistakes can be costly, especially for someone on the margins. And, negative experiences like these may also lead many to steer clear of important online services–like online banking, health management tools, or even email. This response, left unchecked, will only serve to deepen economic divides and allow our most vulnerable populations to fall further behind. We have to confront this head on, and I look forward to hearing from this panel on how we might do that. This is not a state or local problem, but a national one–and we should invest accordingly, at the Federal level.

Ultimately, we cannot expect under-resourced, under-staffed state and local governments to defend their networks from state-sponsored hackers from Russia, China, and Iran. Toward that end, I am working on a comprehensive package to improve the cybersecurity posture of our state and local governments. I look forward to hearing from our witnesses today about opportunities to address this important national security issue.

# # #

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