FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson (D-MS)

Examining DHS's Cybersecurity Mission

Subcommittee on Cybersecurity & Infrastructure Protection

October 3, 2017

There is no doubt that our country is facing an evolving array of cyber threats. As we stand here today, our enemies are thinking of new and novel ways to strike at everything from banks to hospitals and chemical facilities. Nefarious actors even want to disrupt some of our most basic institutions.

Last year, we learned that our nation's election system served as a 'new frontier' for cyber attacks.

With every passing day, we learn of new ways cyber operatives are looking to exploit everything from the media we consume to the databases that store voter registration data.

In this country, there is nothing more sacred than the ability to engage in civic activity and cyber criminals are seeking to undermine our democracy.

Furthermore, as I watch the devastation unfold in Texas, Florida, Puerto Rico, and the Virgin Islands – I am reminded of the fragility of our systems. Disrupting the systems we rely on for power, fuel, food and water can be deadly, regardless of whether it's caused by a cyber attack or a natural disaster.

In short, the digital networks we rely on for our day-to-day life are facing a multitude of threats. To respond to these threats, Congress has put its trust in DHS.

Over the past few years, Congress—by way of this Committee—has consistently expanded DHS' cybersecurity mission – giving the Department a key role in securing Federal networks as well as the systems that support our Nation's critical infrastructure.

The Department made huge strides in implementing these new authorities – including by standing up an automated system to share cyber threat data and advising the new Election Infrastructure subsector on how to promote cyber hygiene with election administrators throughout the country.

We cannot, however, expect DHS to carry out these responsibilities with both hands tied behind its back. To be successful, the Department needs adequate resources, a robust staff, strong leadership, and a clear strategy.

Unfortunately, this Administration has been gravely unfocused when it comes to

cybersecurity. President Trump falsely promised to deliver “a comprehensive plan to protect America’s vital infrastructure from cyberattacks” on his first day in office. It took months for the President to get around to issuing an Executive Order on cybersecurity.

Also, a quarter of the 28-person National Infrastructure Advisory Council resigned in protest of President Trump’s “insufficient attention” to cyber threats.

President Trump floated the idea of an “impenetrable cyber unit” with Russia at the same time members of his administration were considering - and ultimately decided - to ban the use of Kaspersky products on Federal networks.

Within DHS, the Chief Information Officer resigned after serving only four months, and the National Programs and Protection Directorate, the Department’s main cyber arm, is still operating without a permanent Under Secretary.

Whether the men and women in this room are willing to acknowledge, in an open setting, that they are struggling without this leadership – we can be certain these gaps are making their jobs harder.

I look forward to hearing from this panel today about how the Department is carrying out its cyber mission, and I hope that you’ll be candid with us about the obstacles you face. If there are areas where you need additional resources or legislative clarity, tell us how we can help.

# # #

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