COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

The Road to 2020: Defending Against Election Interference

November 19, 2019

I'd like to thank Chairman Richmond for calling today's hearing on election security.Since 2016, officials throughout the Intelligence Community have described in disturbing detail the many ways the Russian government sought to meddle in our elections. For the three years that followed, heads of the Department of Homeland Security, the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency, among others, have warned that the Russian government will continue its efforts to sow discord and undermine confidence in our democracy. More disturbing yet, Russia is not alone. According to the 2019 Worldwide Threat Assessment, other adversaries, including China and Iran, will pursue opportunities to interfere in our elections. The Intelligence Community assesses that adversaries could exploit cyber means to target election infrastructure or engage in targeted influence campaigns to manipulate public opinion. We also know that our adversaries will target political campaigns because they have done so in the past. Our adversaries have hardly kept their desire to undermine the integrity of our elections a secret. As Members of Congress, we have a duty to act.

Today, we are less than one year away from the 2020 presidential election. The question everyone on this dais must ask themselves is: "Have we done enough to secure the 2020 elections from our adversaries?" Despite multiple efforts led by the House of Representatives, Congress has yet to send a single piece of comprehensive election security legislation to the President's desk. Instead, good pieces of legislation to provide additional resources to State and local election officials and limit foreign interference have stalled in the Senate. Moreover, despite multiple requests, the White House has failed to identify an official to coordinate the election security activities at various Federal agencies. In the meantime, we have just a handful of legislative days left this year, and only a limited amount of time for legislative action next year. I will be interested to learn from our witnesses how they recommend Congress use that time to improve election security in advance of the 2020 elections.

Importantly, I will be interested to know how academics and the private sector can work with State and local elections officials and campaigns to improve election security in the absence of Congressional action. The election security problems we face are shared, and we have a shared responsibility to solve them. State and local election authorities – with help from the Federal government – must invest in IT departments, train their employees, and upgrade and certify their election equipment. The private sector, including voting system vendors, must take responsibility to secure their equipment, make it user-friendly, and demonstrate a willingness to admit weaknesses in their systems when examined by third-party cybersecurity professionals. Political campaigns must step up, too. They must implement robust cybersecurity policies to deprive our adversaries of information that can be twisted into a divisive narrative and serve as an extra check on disinformation.

Finally, the American public must also be vigilant, and scrutinize the information presented to them carefully. Before I close, I would also like to note that November is Critical Infrastructure Security and Resilience Month. I can think of no better way to observe it than to assess our preparedness for the 2020 Presidential elections.

# # #

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