FOR IMMEDIATE RELEASE

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

A Borderless Battle: Defending Against Cyber Threats

March 22, 2017

Cybersecurity is at the forefront of American politics in a way that, in my 24 years in Congress, I have never seen.

On this Committee, we regularly gather to hear from cybersecurity leaders on the most pressing security vulnerabilities to our Nation and the novel ways our enemies seek to exploit them.

This past fall, details began to emerge about an entirely new attack vector—a hacking campaign designed to impact the presidential election.

Even before the election, Secretary of Homeland Security Jeh Johnson and Director of National Intelligence James Clapper warned that Russian President Vladimir Putin directed hackers to penetrate the email accounts of high-ranking Democratic officials to acquire information for the purpose of embarrassing and undermining the candidacy of Secretary Clinton.

We may never know whether the Russian intervention was the determining factor in such a close election. Still, Congress has a responsibility to address the unanimous determination of our Intelligence Community that Putin's government successfully meddled in our democracy and, in the view of the IC, will do so again.

In fact, in response to a question about the risk of future Russian hacking against our election systems, FBI Director James Comey said "they'll be back."

The full scale of this state-sponsored hacking campaign is still not fully known, but what we do know is that in addition to hacking private email accounts of prominent Democrats, the Russian hackers tried infiltrate vital networks and equipment maintained by State election authorities.

The Russian cyber campaign sought to strike at the heart of our democracy. As such, legitimate questions about contacts between President Trump's inner circle and associates of the Putin regime need to be brought to light.

That is why I support an independent 9/11-style commission to investigate the Russian cyber campaign. For our part, this Committee needs to do aggressive oversight into this matter.

It is disheartening to see President Trump be dismissive about investigating this very significant cyber attack, even as DHS and its Federal partners work to raise the level of cyber awareness and hygiene across the country.

Just this week, President Trump, responding to testimony from the FBI and NSA before the House Intelligence Committee that laid bare that there is no truth to the President's allegations that former-President Obama "tapped his wires," tweeted "the Democrats made up and pushed the Russian story."

If this was all "fake news" then why would FBI Director Comey be dedicating scarce resources, since July, to investigating the Russian government's interference with our election and "any links between individuals associated with the Trump campaign and the Russian government"?

What seems to be lost on President Trump who, during the campaign, repeatedly expressed support for DoD using cyber offensive capabilities is that there can be no retribution without attribution.

I am pleased that we have with us today cybersecurity leaders who understand the dangers posed by state actors like Russia and can speak to what we should be doing inside our government and with our allies, including NATO, to protect critical infrastructure, including election infrastructure.

Before I yield back, I must express my deep concern about the aloof, bordering on belligerent, posture taken by the Trump Administration with respect to our NATO allies. Last week, the President not only repeated an unsubstantiated Fox News claim that defamed the UK intelligence service but, when asked by German Chancellor Merkel to shake her hand at a White House press event, refused.

This week, we hear that his Secretary of State will not be attending a long-scheduled NATO meeting but plans to visit Russia in April. At a time of heightened threat to Europe, it is critical that the Trump Administration reverse course and reassure our NATO allies that we are full partners against all threats—be they cyber or conventional.

# # #

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