



COMMITTEE ON
**HOMELAND
SECURITY**
DEMOCRATS

Rep. Bennie G. Thompson, *Ranking member*

FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson (D-MS)
***The Current State of DHS Private Sector Engagement for
Cybersecurity***

Subcommittee on Cybersecurity & Infrastructure Protection

March 9, 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, the Secretary of Homeland Security and the Director of National Intelligence warned that Russian President Vladimir Putin directed hackers to penetrate the email accounts of high-ranking Democratic party officials to acquire information to be used to embarrass and undermine the candidacy of Secretary Clinton.

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.

It has been disheartening to see President Trump display a somewhat dismissive attitude about 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.

I continue to be troubled by how long it took President Trump to accept the facts presented by the Intelligence Committee about the Russians orchestrating the hacking campaign. What seems to be lost on this man who has repeatedly expressed support for our government using cyber offensive capabilities is that there can be no retribution without attribution.

I am pleased that we have with us today representatives from private sector that know a thing or two about the nature of the evolving cyber threat and the importance of attribution.

I would like to also take a moment to welcome Robyn Greene who this Committee has come to count on for counsel when it comes the privacy challenges associated with cyber information sharing. I look forward to hearing from the panel on how DHS helps private entities secure their networks against intrusion.

#

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

