U.S. Senate Committee on Homeland Security and Governmental Affairs
"Mitigating America's Cybersecurity Risk"

April 24, 2018
Ranking Member Claire McCaskill

Opening Statement

Thank you Mr. Chairman. I appreciate you holding this hearing.

Hardly a week goes by without some type of cyber incident dominating the headlines. As the United States and the world become more digitally connected, I suspect that trend will only continue.

Our government is a lot older than the Internet, so we have had to retrofit technology into existing government structures. But unlike a lot of issues that naturally fit into a single department or agency, cybersecurity and data protection affect all aspects of government. In the last few years, however, Congress, and in particular this Committee, have made a great deal of progress enhancing the federal government's ability to track and improve its cybersecurity.

We codified the Department of Homeland Security (DHS) to coordinate the operational security of federal systems. That included designating DHS as the hub for information sharing, running the intrusion prevention and detection programs that are now mandated throughout federal departments, leading asset response activities, and coordinating the protection of critical infrastructure. When

necessary, DHS also has the unique authority to direct another agency to take certain steps to protect its systems.

While every department and agency is ultimately in charge of protecting its own systems, Congress has done a lot to make DHS the primary cyber coordinator for the civilian federal government. This hearing is an opportunity to assess how DHS is using the authorities Congress provided and if those tools are measurably improving agencies' awareness and security.

As I mentioned, part of DHS's responsibilities also include coordinating critical infrastructure protection, but the majority of critical infrastructure is not federally owned or operated. That is certainly the case with election systems, which are owned and operated by states and localities.

We all know that the Intelligence Community assessed with high confidence that Russia launched a campaign to influence the 2016 election, part of which aimed to undermine public faith in the U.S. democratic process. A component of that operation included attempts to hack into voter registration systems.

In the months before the election, DHS stepped up and offered cyber assistance to states that wanted help. And in the aftermath of the election, DHS designated election infrastructure as critical infrastructure, which enabled interested states and localities to jump toward the front of the line to receive that help.

In the roughly two years since this issue appeared on the radar of states and the federal government, DHS has made progress building relationships with election officials and associated organizations throughout the country, and in helping interested states and localities assess and improve the security of their voting systems. There have certainly been some bumps in the road, but I think DHS is on the right track. That said, I have serious reservations about our level of preparedness. Just last week, DHS Secretary Nielsen declined to express confidence in the country's election security, admitting only that there is increased awareness of the threat. I find that troubling.

Beyond that, I am concerned that this Administration has only been treating the symptoms of Russia's interference. U.S. policy towards Russia has been uneven at best, and at worst, I worry that we have done little if anything to actually change Russian behavior and stop them from trying to undermine our institutions and democracy.

I look forward to hearing our distinguished witnesses' assessments of our cyber and election security and how we can improve it in the future.

Thank you, Mr. Chairman.