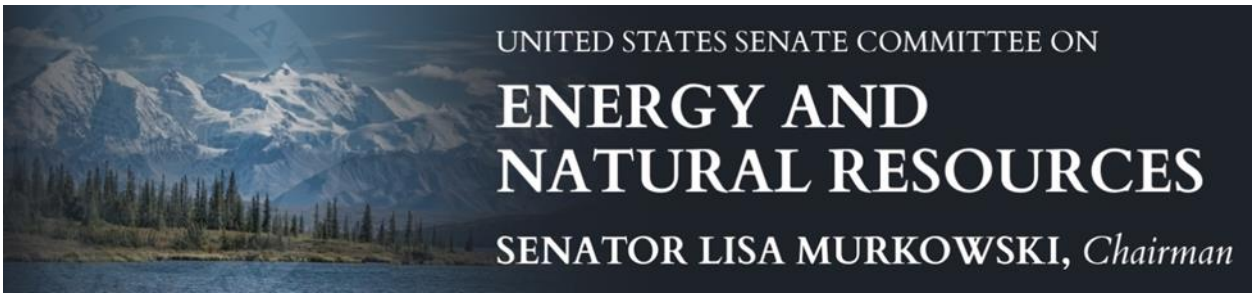

Opening Statement
Oversight Hearing on Advanced Cyber Technologies
Chairman Lisa Murkowski
October 26, 2017

Good morning, everyone. The committee will come to order.

Over the years, we have conducted a number of hearings designed to examine the vulnerabilities of our nation's electric grid system. In this Congress, we have held a series of hearings focused on cybersecurity, electromagnetic pulse, and grid security issues at both the full committee and the subcommittee levels.

During today's hearing, we will add to that by looking at advanced and emerging cyber technologies and processes that are being developed in our national labs and in the private sector. These are technological improvements—and sometimes breakthroughs—that could be used to protect the grid, as well as other critical energy infrastructure, from future cyberattacks.

I have mentioned certainly many times in this committee, but outside the committee as well, that around the country sometimes we get the sense that folks believe in this "immaculate conception" theory of energy—that it just happens. We all recognize there is a lot more to it, than that. But a related question is, what happens when the lights don't turn on? When you flip that switch and you just expect it to happen, and then they're not there. What happens when electricity is out for an extended period of time? We are certainly seeing in Puerto Rico right now and the U.S. Virgin Islands the real world impact of an extended power outage.

Just as we can harden our energy infrastructure to protect it from natural disasters, we must also look to ways to harden the grid from constantly-evolving cyber intrusions, as well. It seems like every day now we hear about an attempted hack or actual breach that has taken place, and the list is long and getting longer—OPM, Ukraine's power grid, the WannaCry ransomware, Equifax, Anthem, Home Depot, Target…the list keeps growing and growing. Just last Friday, the Department of Homeland Security issued a public alert of an ongoing hacking threat to U.S. energy systems.

In the midst of all of this, we have to continually look for ways to eliminate, diminish, or mitigate our vulnerabilities. Whether it is the application of quantum encryption, artificial intelligence, or moving control of grid infrastructure off of the public internet, the witnesses we have today will help provide our committee with insights into how we can protect our national energy infrastructure now and into the future.

I mentioned quantum encryption, and I would like to note a recent article by McClatchy about the advances China has made on the topic. Earlier this year China announced that a satellite and ground station 745 miles apart had communicated through quantum particles. Last month a video conference between China and Austria – a distance of 4,600 miles – was held via China's quantum satellite. They've established a 1,200 mile quantum link between Shanghai and Beijing and announced that they will build a $10 billion quantum research facility.

According to that article, some scientists believe that with the amount of resources China is putting into the field, a quantum computer may be built in a decade or less. Whether these claims are accurate remains to be seen, but it is clear that significant research is underway around the world in the cyber realm.

I want to thank our witnesses for joining us today and look forward to learning about their efforts to combat this threat, particularly on the work they are doing to help keep our electric grid and energy infrastructure safe and reliable.

I'll now turn to Senator Cantwell for her opening comments. And I want to thank you, Senator Cantwell, because you have been dogged and persistent when it comes to the issue of cyber and cyber threats, particularly as they relate to our energy grids.

###