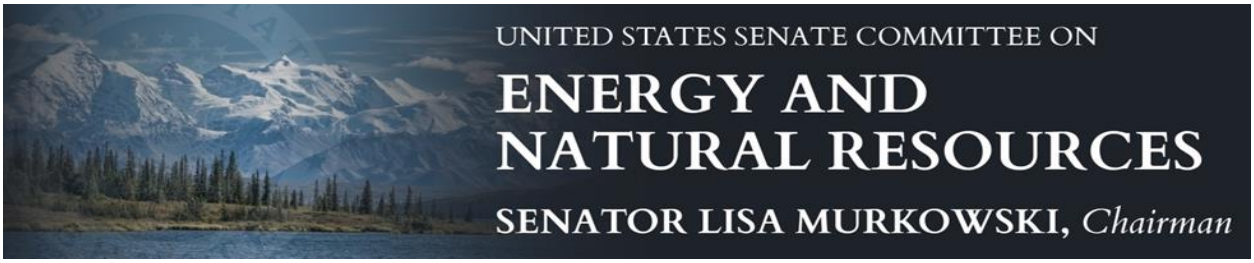

Opening Statement
Full Committee Hearing on Cyber Security and Resiliency
Chairman Lisa Murkowski
March 1, 2018

Good morning. The committee will come to order, as we begin our hearing on the cybersecurity and resiliency of our critical energy infrastructure.

Cyberattacks are a well-documented and continuing threat. Every day we seem to hear of yet another incident. Increasingly, it appears that the bad actors are nation-states and sophisticated entities, such as organized crime or terror groups. These attacks are across-the-board and not limited, of course, to energy infrastructure.

Just last week, according to news reports, U.S. intelligence identified efforts by Russian military spies to attack computers used by Olympic officials during this year's games. Reportedly, their goal was to make it look as if North Koreans were leading the cyberattack. Acts of cyber intrusion such as these can jeopardize diplomatic relations and could have more serious repercussions.

Just a couple days ago, the Director of the Division of Elections in my home state of Alaska again informed the public that Russian cyber actors made a failed attempt to access the Division's public website prior to the 2016 election. Apparently, they merely scanned the state's system – this wasn't a 'breaking and entering' scenario – but it clearly underscores the persistence of the problem.

Here in the United States, the energy sector is clearly a high value target for cyber-attacks. Earlier this month, Entergy's security monitoring system detected a cyber-intrusion on the company's corporate network. Thankfully the intrusion was on the corporate side and did not affect energy delivery or reliability, but again bad actors will test any available avenue in an attempt to infiltrate energy networks.

Our Committee has spent a lot of time, many hours examining the threats to energy infrastructure. We have learned about the potential challenges of increased digitalization of the energy sector, and opportunities to improve cybersecurity by engineering in protections and developing strong cybersecurity protocols. We have repeatedly heard how protection of our nation's critical assets is a shared responsibility, with federal, state, and private sector partners working together to improve cyber defenses and sharpen responses to cyber-attacks. We know there is more work to be done to improve that collaborative work. We are alert to the danger that

"shared responsibility:" can, in practice, be the hardest responsibility to consistently and accountably discharge.

We have also legislated to help address the cyber-security problem. In the Energy Policy Act of 2005, Congress imposed mandatory reliability standards, including cyber standards, on the electric industry. Today we will hear testimony that these standards have led to meaningful improvements. The electric sector is still the only sector that has such stringent requirements. But we will also hear that keeping the nation safe from major cyber threats goes well beyond regulation.

Last Congress, in the FAST Act, we enacted provisions authored by this committee to codify the Department of Energy as the sector-specific agency for the energy sector and provide the Secretary with authority to address grid-related emergencies, including cyberattacks. We also sought to facilitate greater information sharing by protecting sensitive information from disclosure. I am pleased to report that public and private sector efforts, not only to identify threats and share information but also to improve the capabilities for detecting and responding, are intensifying.

So the question this morning is "What is next?" – What should the federal government do (or refrain from doing) to meet this dynamic and evolving threat? How can government help improve the cyber resiliency of critical energy infrastructure if a threat becomes a reality?

Mr. Walker's testimony states that Secretary Perry "is establishing" a distinct "Office of Cybersecurity, Energy Security, and Emergency Response." This new office, which will be known by the acronym C.E.S.E.R., we're already referring to it I guess as CAESAR (big shoes here). But much of CESER's lineage is from the Department's current office, the Office of Electricity Delivery and Energy Reliability, which was established after the 2003 Northeast Power Blackout. Mr. Walker, we appreciate the Department's attention to this important topic and certainly look forward to learning more about the new office, and how you intend it operate and function.

Protecting our nation's energy infrastructure, we all agree, is critical to maintaining so much of the American way of life. We must determine what the next appropriate steps will be to further identify and prevent cyber intrusions and increase resiliency in the event of an attack. Those solutions may not require more regulation, but rather more common sense and cooperation.

I appreciate each of our expert witnesses that we have before us today, making the time to testify before our committee, and I will introduce them after Senator Cantwell's opening remarks, but we appreciate you being here. Senator Cantwell.

###