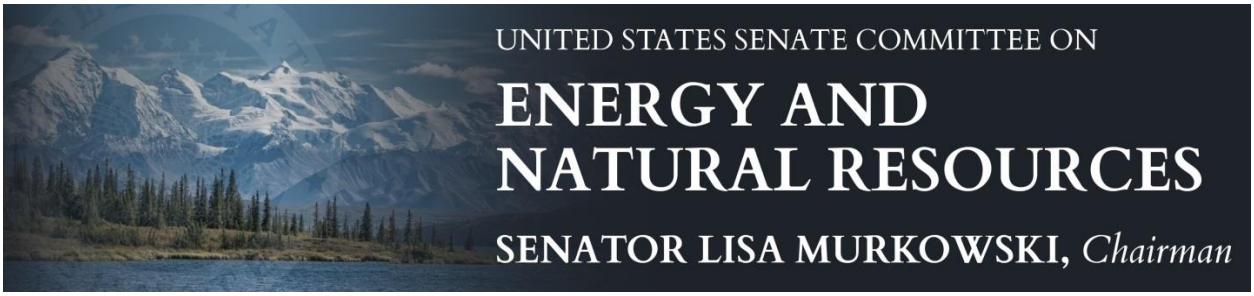

Opening Statement
Full Committee Hearing on Cybersecurity Efforts in the Energy Industry
Chairman Lisa Murkowski
February 14, 2019

Good morning. The committee will come to order.

I will just note for the record that today is Valentine's Day, some celebrate it with flowers and chocolates. Here at the Energy Committee what we prefer to do is take a deep dive into the very real cyber threats that face our electric grid system. So, here's the punchline everyone, hold on – after all, nothing says love like ensuring the security of critical energy infrastructure. So that's our Valentine's statement for the morning from the Energy and Natural Resources Committee – you've got to love the script writers back here.

Last week we had a chance to examine the state of energy markets and the promise of clean energy innovation. Both of those hearings, great hearings by the way, highlighted the increased automation and digitalization of energy technologies. While advances in technology are always welcome, always welcome, and can help us run things more efficiently, each new digital connection also opens a potential pathway for bad actors to disrupt our energy delivery.

We know that the threat of cyber attacks by our foreign adversaries and other sophisticated entities is real and growing. Last month's 2019 Worldwide Threat Assessment detailed how China, Russia and other foreign adversaries are using cyber operations to target our military and our critical infrastructure. The assessment notes that our electric grid and natural gas pipelines are particularly vulnerable to attack and that Russia is mapping our infrastructure with the long-term goal of causing substantial damage.

Unfortunately, we have already seen the real world ramifications of cyber attacks on energy infrastructure. Back in December 2015, Russian hackers cut off power to nearly a quarter-million people in Ukraine. And in the summer of 2017, Russian hackers infiltrated the industrial control system of a Saudi Arabian petrochemical plant and disabled the plant's safety systems.

We know we don't want that to happen here. We cannot let it happen in the United States. Our grid system is 'uniquely critical' and the consequences of a successful cyber-incursion would be widespread and potentially devastating. The resulting loss of power would impact hospitals, banks, cell phone service, gas pumps, traffic lights – you name it.

The government's focus on cybersecurity, in partnership with industry, is a major reason that the United States has not experienced an attack like Ukraine's. In the 2005 Energy Policy Act, Congress created the Electric Reliability Organization – we have since certified it as NERC –

and mandated reliability standards to be developed through an industry stakeholder process. Protecting our nation's critical assets is a shared responsibility, with federal, state, and private sector partners working together to improve cyber defenses and coordinate responses to cyber attacks.

The 2015 FAST Act enacted provisions authored by this committee to codify the Department of Energy as the cyber sector-specific agency for the energy sector and provide the Secretary with authority to address grid-related emergencies. We also sought to facilitate greater information sharing by protecting sensitive information from disclosure.

The Administration is also taking steps to address emerging cyber threats. Last year the Department of Energy established the new Office of Cybersecurity, Energy Security, and Emergency Response, also known as "CESER." I look forward to learning more about the work being done by this office, Assistant Secretary Evans has been on the job for about six months here, so gaining your perspective this morning is going to be very useful for us.
The Department is also partnering with FERC to find solutions to energy infrastructure threats. Next month the agencies will co-host a technical conference to discuss current and emerging cyber and physical security threats, as well as ways to incentivize cybersecurity investments. So, I think it's very important that we're seeing these agencies assigned this top priority of cybersecurity and plan this conference very closely together.

I'm pleased to welcome a very distinguished panel this morning. We have from the Federal Energy Regulatory Commission, Chairman Neil Chatterjee, we appreciate your leadership at the Commission and look forward to your comments this morning. I mentioned the Assistant Secretary at the Department of Energy working in CESER, Karen Evans. From the North American Electric Reliability Corporation, we have Mr. Jim Robb, let's just call it NERC. We have David Whitehead from Schweitzer Engineering Laboratories and we have Major William Keber from the West Virginia National Guard Critical Infrastructure Protection Battalion.

So I think it's well recognized that the panel we have all represent those who are at the frontlines of the effort to protect our energy infrastructure from cyber threats. Thank you for being here and I look forward to your testimony and comments. I will now turn to my Ranking Member, Senator Manchin.

###