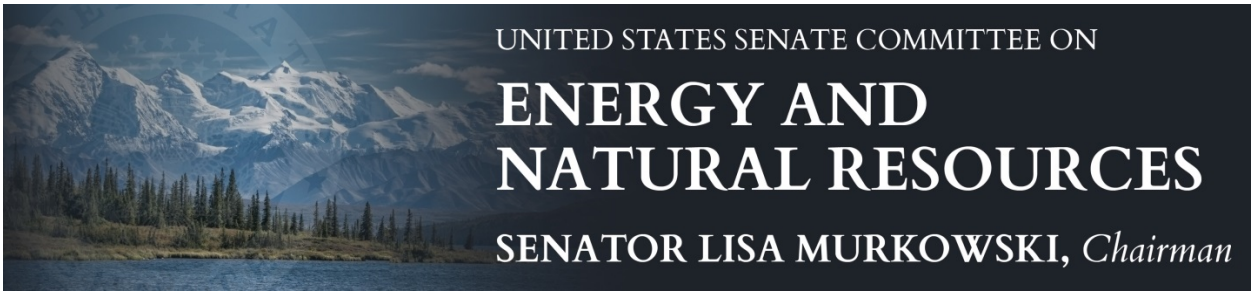

Opening Statement
Full Committee Hearing on Cybersecurity in the Energy Industry
Chairman Lisa Murkowski
August 5, 2020

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

We are here this morning to examine federal and industry efforts to improve the cybersecurity of the energy sector, including efforts to improve collaboration on various cybersecurity and critical infrastructure protection initiatives.

It has been more than a year since we last held a hearing on cybersecurity for the energy sector, but I think it's fair to say that this is always a timely topic. It's also a critical priority that we can't lose sight of, even as we grapple with COVID-19, lest it become the source of our next national crisis.

There have been a few noteworthy developments since our last hearing. Earlier this year, the President issued an Executive Order focused on securing the bulk power system from both cyber and physical threats posed by hostile nation-state actors, this is an effort that will be led by the Department of Energy. Meanwhile, the Federal Energy Regulatory Commission has published a paper detailing a potential structure for providing incentives to utilities to make cybersecurity investments, following up on a technical conference examining the same issue in 2019.

I'm pleased this morning to be able to welcome our witnesses from DOE and FERC and look forward to hearing the latest from them. I also welcome the witnesses representing industry, which will play an equally significant role in how these initiatives unfold.

The threat of cyberattacks by foreign adversaries and other sophisticated entities is real and it's growing. As I mentioned on the Senate floor earlier this week, when we confirmed Mark Menezes to be Deputy Secretary of Energy, cyber-attacks are near-constant and only growing more sophisticated.

According to the latest Worldwide Threat Assessment from the Office of the Director of National Intelligence, China, Russia and other foreign adversaries are using cyber operations to target our military and our critical infrastructure. Those near-peer adversaries already have the capability to launch cyberattacks against electric and gas infrastructure.

The COVID-19 pandemic has created a unique opportunity for cyber criminals to attack our networks, including critical energy infrastructure. The Department of Justice recently issued a press release announcing the indictment of two individuals backed by the Chinese Ministry of

State Security. DOJ noted these two individuals not only targeted portions of our energy sector, including DOE's Hanford site, but also entities conducting research on a coronavirus vaccine.

We cannot allow hostile foreign nations to disrupt our way of life. Energy is the lifeline for all critical infrastructure sectors, and protecting our critical infrastructure is the first step in ensuring its continuity.

Unfortunately, we've already seen the real-world ramifications of cyber-attacks on energy infrastructure, and this is most vividly in Russia's attacks on Ukraine.

In December of 2015, Russian hackers cut off power to nearly a quarter-million people in Ukraine in an attempt to disrupt and intimidate. 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. More recently, an advanced Russian government-backed hacking group is alleged to have probed a U.S. energy entity's network, according to a release that DOE issued in January.

We all know the stakes here. A successful hack could shut down power – impacting hospitals, banks, gas pumps, military installations, and cell phone service. The consequences would be widespread and devastating, and only more so if we are in the midst of a global pandemic.

The federal and industry focus on cybersecurity is a major reason why the United States has not experienced an attack like Ukraine's. Protection of our critical assets is a shared responsibility, demanding that federal, state, and private sector partners work together to improve cyber defenses and coordinate responses to cyber-attacks.

The FAST Act of 2015 contained provisions authored by our committee to codify the Department of Energy as the sector-specific agency for the energy sector and to provide the Secretary with authority to address grid-related emergencies. We also sought to facilitate greater information sharing by protecting sensitive information from disclosure. Our American Energy Innovation Act also has numerous sections to enhance government-industry partnerships in this space and establishes programs to enhance the cyber posture of [smaller] utilities.

Most recently, I introduced a new bill, the Energy Infrastructure Protection Act, to update provisions in the Federal Power Act and restrict federal disclosures of certain sensitive energy information. I know that there are a few who may disagree with that approach, but the alternative – disclosing and displaying our vulnerabilities for our enemies – will hardly make us any safer.

I'm pleased to welcome a distinguished panel of witnesses who are truly at the frontlines of the effort to protect our energy infrastructure from cyber threats. So, I thank you again for being with us this morning.

I'll now turn to my colleague and Ranking Member, Senator Manchin, for his opening remarks.

###