Statement of Chairman Frank Pallone, Jr.
House Energy and Commerce Committee
Subcommittee on Energy
Hearing on "Keeping the Lights On: Addressing Cyber Threats To The Grid"

July 12, 2019

Thank you, Chairman Rush, for holding this hearing today on the very important topic of cybersecurity of our nations electric grid. We know our enemies are rapidly developing new techniques to compromise and attack our grid. It is important government and industry stay on top of the issue.

I know our witnesses and their agencies - the Department of Energy, the Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation - all take cybersecurity of the grid very seriously and are doing good work. I look forward to today's discussion.

I am pleased Secretary Perry established the Cybersecurity, Energy Security, and Emergency Response, or CESER (/*Cesar/*) office, to focus specifically on these pressing issues. Chairman Rush and Mr. Walberg have introduced bill H.R. 362, the Energy Emergency Leadership Act, to enshrine in statute this new focused level of leadership at the Department of Energy. I hope we are able to report this legislation out of the full committee soon.

This bill, along with three other bi-partisan bills addressing cybersecurity of our nation's energy systems, were favorably forwarded to the full committee recently. These bills are a top priority to move, and I am very proud of our strong bipartisan working relationship and the committee's efforts on cybersecurity.

We all understand time is of the essence. March 2019 marks a sobering milestone of the first reported malicious cyber-event that disrupted grid operations of a Western utility. Thankfully, there seemed to be very little effect to the transmission grid and no resulting blackouts. We must stay ahead of our enemies and keep it that way.

I appreciate FERC and NERC's work together to continue enhancing Critical Infrastructure Protection Standards like the final rule last October to bolster supply chain risk management. This rule implements new reliability standards that respond to supply chain risks like malicious software by requiring responsible entities to develop and implement security controls for industrial control system hardware, software and services. These are the types of important forward-looking actions we need to proactively protect our grid against attacks.

And, while this hearing today is not about cybersecurity relating to our pipelines, I'd be remiss not to mention how important that is to our grid system. We have a reliable pipeline system, but we never want to find ourselves in a different situation. DOE, FERC, and NERC's responsiveness to the committee's briefing request and job of oversight is a welcomed change from the stonewalling from TSA who refuse to testify. As I've said before, and my friend from Michigan, Ranking Member Upton has echoed, if TSA does not want to be taken seriously, we may have to look at other options.

I want to thank our witnesses for being here today. I look forward to hearing about CESER's range of work including work on a national strategy and cybersecurity risk assessment of the grid. I also looking forward to hearing about FERC and NERC's continued work to build out a critical infrastructure cybersecurity framework. In general, how are you working to incentivize and implement leading cybersecurity standards? What types of collaborative processes are your agencies working on with industry? And, what can congress do to support each of your agencies work?

Thank you, I yield back.