Opening Statement
Chairman Frank Pallone, Jr.
Committee on Energy and Commerce
Subcommittee on Energy
Hearing on “Keeping the Lights On: Addressing Cyber Threats to The Grid”
July 12, 2019

Today we are here to get an update from federal agencies about how they are addressing cyber threats to our electric grid. We know our enemies are rapidly developing new techniques to compromise and attack our grid, so it is vitally important that the federal government and the electric industry remain vigilant in ensuring the grid is secure.

Our Committee has been conducting robust oversight on this important topic in a bipartisan fashion for years. Today’s hearing is a public forum to discuss how the Federal government is addressing cybersecurity challenges, but the Committee also continues to receive closed-door briefings on the issue to understand more classified matters.

Our witnesses and their respective agencies all take cybersecurity of the grid very seriously. And I believe Secretary Perry made the right decision in creating the position of Assistant Secretary for Cybersecurity, Energy Security and Emergency Response to focus specifically on these pressing issues.

Last month, this Subcommittee favorably reported out legislation introduced by Chairman Rush and Mr. Walberg that would enshrine in statute this important new division at DOE. I look forward to bringing this bill and three other bipartisan cybersecurity bills up for a markup at the full Committee soon.

We must be both active and vigilant when it comes to cybersecurity because time is of the essence. In March, we had the first reported malicious cyber-event that disrupted grid operations of a Western utility. Thankfully, there seemed to be very little effect on the transmission grid and no customers lost power. But we must stay ahead of anyone who is a cyber threat.

I appreciate the work of FERC and NERC 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 specifically about pipeline cybersecurity, 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. I remain concerned about the lack of resources and expertise at the Transportation Security Administration’s (TSA) Pipeline Security Program. I look forward to hearing from DOE about possible ways they could help address these safety gaps. As I’ve said before, if TSA continues to devote scant resources or attention to these matters, we must start looking at other options to keep our pipes secure.

I thank our witnesses for being here today as we discuss this critical security issue, and I yield back.