Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Full Committee Ranking Member Frank Pallone, Jr.

Hearing on "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid"

December 2, 2025

I'm pleased the Subcommittee is holding this important hearing today, as cybersecurity is a critical issue that can impact energy affordability and reliability.

This is also the first Energy Subcommittee hearing this Congress that was put together in a bipartisan way. It is December – we should be having hearings like this regularly rather than annually.

Securing our nation's energy infrastructure from cyber and physical threats should be something we can all agree on. After all, threats to our energy systems are only growing, whether it be from nation-state actors such as Russia or China, or domestic terrorists here at home, whose capabilities are being enhanced every day by increasingly effective artificial intelligence tools. Soon, attacks that would have required the resources of a sophisticated opponent will be able to be carried out by a single person. And our adversaries with resources will be able to sow chaos on a much larger scale than we ever anticipated.

These threats are not hypothetical. Earlier this year, we discovered that hackers associated with the Chinese government unleashed an attack that compromised the systems of a Massachusetts utility for nearly a year. I don't have to tell anyone the disaster that this could cause – both for the reliability of energy systems and for our mission to keep utility bills low.

That is why today's hearing is so important. While we have discussed the many threats facing energy reliability this year – from President Trump's attack on clean, cheap energy, to threats brought by extreme climate-fueled weather events, to challenges from data centers consuming enormous amounts of electricity – cyber threats to the grid involve an adversary who will seek to overcome any barriers we can raise against them. We must be in a state of constant evolution.

The interconnected nature of our energy systems means that any one threat cannot be viewed in isolation. Threats to a gas pipeline can quickly cascade into a threat to electric reliability. And because of this interconnectivity, we must ensure that experts from the Department of Energy play a key role in our government's cybersecurity defenses for the energy sector.

While agencies under the Department of Homeland Security can play an important convening role, it is DOE, not Homeland Security, that has the critical relationships with all the relevant actors in the industry, and has the expertise necessary to view threats in a holistic manner. We saw this in the aftermath of the Colonial Pipeline cyberattack when DOE took the lead on the federal response. I look forward to hearing about some of the work that DOE is doing in bringing together the energy industry to talk about threats that impact everyone.

However, none of this works at DOE unless the agency is properly staffed and has the resources to fulfill its mission. DOE lost more than 3,500 staff this year as a result of Secretary Wright and DOGE's

reckless and relentless attacks on federal workers. We need to ensure that we have sufficient staff working on cybersecurity at DOE, and that they get the resources and funding they need.

When I was Chair of this Committee in 2021, we passed a law establishing a number of cybersecurity programs at DOE and the Federal Energy Regulatory Commission (FERC). Many of those programs are now coming up for reauthorization, and are ripe for examination to see what worked, what didn't work, and lessons we should all learn as we look to potential legislative action.

Finally, I hope we can also discuss the security not only of our energy infrastructure, but of the supply chain that creates that infrastructure. During the last ten months, the Trump Administration has hobbled our efforts to reshore manufacturing in America, increasing tariffs and slashing tax credits that were designed to make American manufacturing competitive. As a result, we are more dependent than ever on foreign sources for critical infrastructure components – a vulnerability that could turn into a devastating weakness if we do not work to reverse it. I hope to hear ideas on how we can turn this around today.

Thank you, Mr. Chairman, and I yield back the balance of my time.