AFFORDABLE ENERGY COALITION

U.S. Electricity Grid & Cyber Security

Background

Over the past year, the administration has sought various ways to economically support coal and nuclear plants. To achieve this, a recently leaked internal White House memo suggests the closure of coal and nuclear power plants leaves the nation's electricity grid more vulnerable to cyber attacks.

What Does Cyber Security Have To Do With The Energy Sector?

Along with other critical infrastructure industries like transportation and healthcare, the energy sector has increasingly become the target of cyber attacks. In a recent March report, the FBI and Department of Homeland Security noted that numerous cyber actors have attempted to infiltrate a wide of variety U.S. energy and utility facilities. As the sector directly responsible for ensuring the country's lights stay on, any cyber attack that could effectively curtail the country's power generation capabilities presents a serious issue policymakers must work to address

What Is The Administration Saying?

As the administration seeks to justify the use of national security laws to prop up uneconomic power producers, they have suggested coal and nuclear plants, with onsite fuel, are significantly less susceptible to cyber attacks than any other class of electricity generators. Without these plants, the administration argues, the U.S. grid will become too reliant on natural gas, whose infrastructure it asserts is at greater risk to cyber threats than the rest of the industry. In his recent remarks, Energy Secretary Rick Perry asserted that the specific closure of "fuel secure" coal and nuclear plants will threaten the grid's ability to bounce back from serious cyber attacks.

Why Are They Wrong?

The truth is, there is nothing about onsite fuel capacity that make coal and nuclear plants less susceptible to cyber threats.

While cyber security is an important priority for the energy industry as a whole, coal and nuclear plants simply do not possess any special attributes that make them less susceptible to cyber threats. The truth is there is nothing about onsite fuel capacity that would shield a power plant's digital technology and operating systems from infiltration. All electricity generators are also equally affected by any attempt to destabilize the nation's overarching transmission infrastructure, which plants rely on to bring their electricity to customers across the country.

The ongoing digitization of the nuclear industry has recently left more reactors at risk, and hackers have in the past sought to penetrate various nuclear facilities around the country. Physical and cyber attacks on the coal industry's supply chain pose additional threats to plants' fuel security.

The Bottom Line?

If the White House is interested in addressing the nation's cyber security threats, they should work with industry leaders and experts to advance sector-wide cyber security solutions.

The administration's emergency directive has absolutely nothing to do with protecting the energy industry from cyber threats, and everything to do with special interests looking to leverage their influence to win a federal bailout.