Testimony to Homeland Security, Public Safety & Veterans' Affairs

Interim Charge: Protecting Texas Critical Infrastructure from Foreign Adversaries

Judd Messer | Advanced Power Alliance | July 30, 2026

Good afternoon, Chairman Hefner and members. For the record: Judd Messer, testifying today on behalf of the Advanced Power Alliance.

APA represents energy developers, owners, and operators invested in power generation projects throughout ERCOT, SPP, and the Southeastern United States.

APA members have invested close to $200 billion here, mostly in rural Texas, leading to over 230,000 jobs. Our members pay about a billion dollars per year in both landowner payments and local taxes and contribute to grid reliability and affordability by adding new generation at an unprecedented pace while providing the lowest-cost electricity available in today's market.

I appreciate you having me here today to discuss a topic of such critical importance for our industry and the electric grid, but also to nearly every sector of critical infrastructure, from energy and telecommunications to transportation, advanced manufacturing, and even our national defense systems.

As you've already heard today, entities registered to participate in the ERCOT market must comply with the Lone Star Infrastructure Protection Act – one of the nation's leading state-level frameworks for protecting critical infrastructure.

LSIPA requires market participants to report purchases of critical electric grid equipment or services from companies with specified ties to China, Iran, North Korea, Russia, or any other country designated by the governor, and to attest that those purchases will not give such companies prohibited access to or control of their equipment.

APA members take those compliance obligations seriously.

We also understand that while country of origin is certainly a relevant risk indicator, it is not a complete cybersecurity standard. Operational risk

also depends on connectivity, remote access, monitoring, and the consequences of any given compromise.

That brings me to the central point I hope to leave with the committee today: that strong cybersecurity and supply chain policy begins by identifying where the greatest vulnerabilities exist and addressing those first.

Imagine I get home this evening. I've had dinner, put my daughter to bed, and it's time to lock up the house. My immediate concern is making sure no one can get inside tonight. So, I'm going to lock the doors and set the alarm.

Now, I may prefer stronger doors and windows, but I can't get them right away, much less before I lay down to sleep for the night. But that doesn't mean I'd remove them now and leave myself and my family more exposed – I'll still lock them and make sure only I have the keys.

The same principle applies to the subject of this hearing.

Cybersecurity controls are the locks and alarms. They protect the hardware and software that actually communicate with the outside world. They address today's most urgent vulnerabilities, can be implemented immediately, and will always remain a critical security control.

Expanding our domestic supply chain is the longer-term proposition, like replacing my doors and windows—this requires national trade and industrial policy, and is not as immediately actionable, nor will it eliminate the need for robust cybersecurity protections.

Fortunately, the United States is beginning to accelerate its domestic manufacturing capacity for this industry, and no state is doing more than Texas, where 73 manufacturing facilities are currently operating and another 15 are under construction or announced for the future.

With that background, I'd like to leave you with three principles to consider as you wade through what a state-level policy of this kind may look like:

1. First, keep requirements technology-neutral, performance-based, and proportionate to operational risk.
2. Second, focus scrutiny on equipment functionality, operational control, and connectivity—particularly where remote access is possible.
3. Third, allow documented mitigation measures for existing equipment where operators can implement equivalent protections.

These principles will strengthen security without trading one grid risk for another.

By contrast, an outright ban on existing and future non-U.S. components, for example, would create immediate reliability and resource adequacy challenges, increase electricity costs, and weaken our ability to compete in the global race to build the energy infrastructure needed to power the next generation of industry and economic growth.

At the same time, such a ban would do little to address today's most significant cybersecurity risks, because sophisticated adversaries care less about where equipment is manufactured than whether they can gain unauthorized access to it.

These three principles – technology-neutral policy, with a focus on functionality, and allowing for mitigation on existing equipment – allow Texas to lock the doors we have today while we build stronger doors for tomorrow.

I appreciate the opportunity to be here with you today and will do my best to answer any questions.

###