Smart Security for the Texas Grid

Advanced Power ALLIANCE

Securing Texas' power grid is critical, but not all cybersecurity measures are equally effective. **Texas can lead the nation on grid security without sacrificing the competitive energy market that keeps costs low for consumers by focusing on engineering standards and access controls that address real threats.** The FAQ below explains why engineering controls, transparency, and verifiable risk management provide strong, practical security without disrupting the state's energy market.

Q DOES TEXAS HAVE LAWS IN PLACE TO PROTECT THE GRID FROM CYBER THREATS?

A

Yes. Texas has a strong legal framework in place. The Lone Star Infrastructure Protection Act (LSIPA) **requires market participants to disclose foreign-sourced equipment from designated countries and companies and certify that they do not permit unauthorized network-connected access** to critical grid infrastructure by prohibited entities. North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) **requires virtually all utility-scale wind, solar, and storage facilities connected to the bulk power system to comply with federal cybersecurity and physical security standards.** That federal coverage is expanding, not shrinking. NERC's new Category 2 threshold will bring additional mid-sized utility-scale assets into full compliance starting in 2026.

Q ARE FOREIGN-MADE DEVICES THE MAIN THREAT TO KEEPING THE GRID SECURE?

A

No. The real danger is in the software and communications controlling those devices. While supply chain security is important, the primary risks to the grid stem from communications networks and unauthorized access to grid-connected devices regardless of where they are made. **Policies that strengthen cybersecurity and limit unauthorized remote access and control are far more effective than additional supply chain tracing at enhancing grid security.**

Q WHAT PROVEN ENGINEERING CONTROLS EXIST TO IMPROVE GRID SECURITY?

A

Current NERC CIP standards already require vendor remote access controls and other cybersecurity best practices for utility-scale resources interconnected with the bulk power system. Future state policies should avoid duplicating current federal requirements and instead examine whether additional engineering-informed practices could further enhance cybersecurity by building on the strong framework already in place.

Q HOW CAN REGULATORS ENSURE COMPLIANCE?

A

The current LSIPA disclosure and transparency requirements, coupled with engineering-informed cybersecurity best practices, will place the responsibility on developers and facility owners, preserve our competitive energy market, encourage scale and adaptation to the evolving threat landscape, **and create an enforcement record that enables the appropriate authority to act on violations.**

The Advanced Power Alliance and our members share the Texas Legislature's commitment to national security. **For APA's members**, which have committed billions of dollars in long-term capital to Texas, **a secure grid and a sound investment are one and the same. Practical and effective grid security is achieved through engineering controls, transparency, and verifiable risk management.** We look forward to working with policymakers on solutions that build on these principles and avoid unintended consequences that could weaken grid reliability, diminish economic competitiveness, or ultimately undermine our national and energy security.

Securing Battery Energy Storage from Cyber Threats (Brattle/Dragos, 2025)
Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance (Idaho National Lab, 2024)