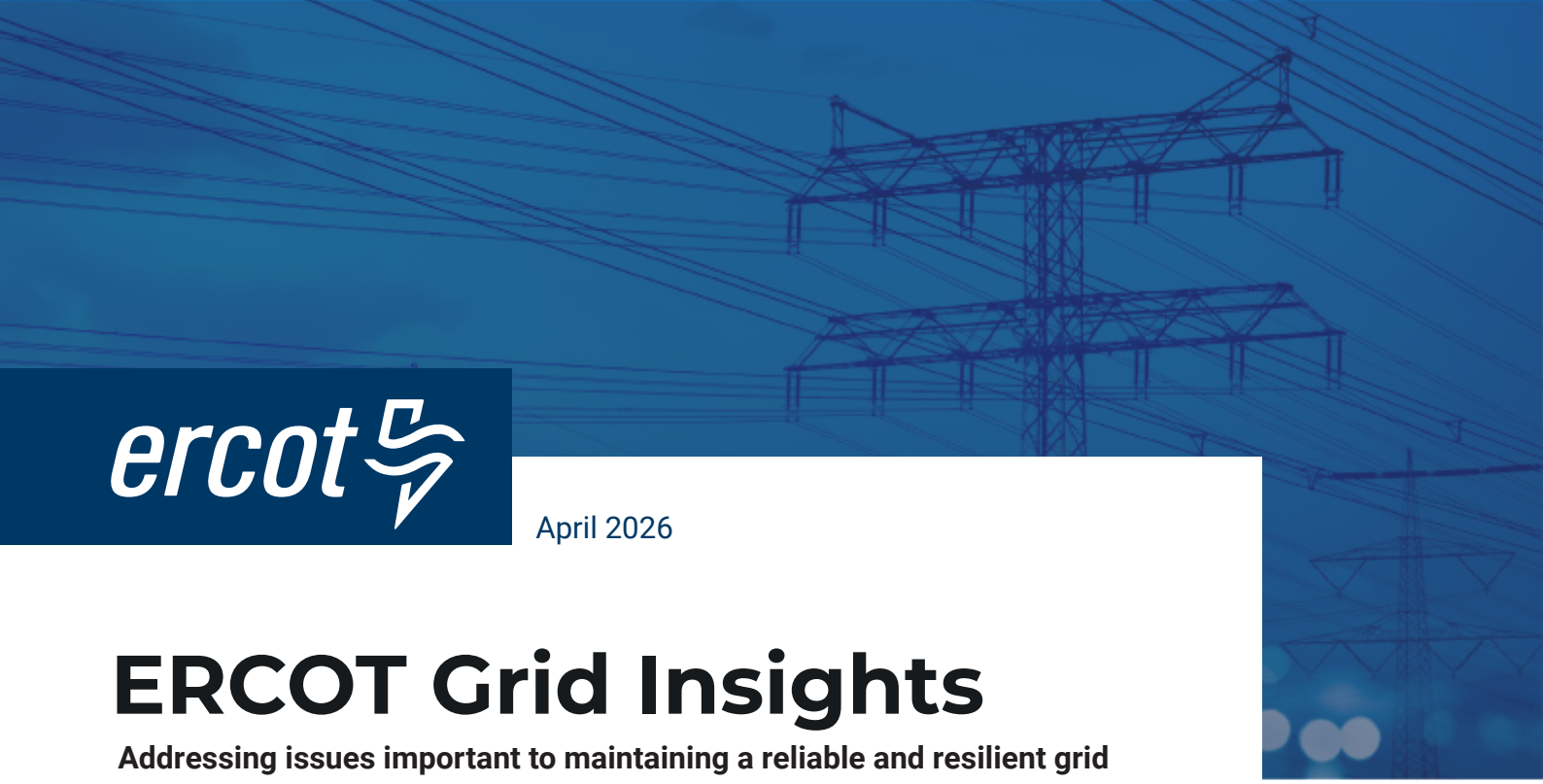


April 2026

ERCOT Grid Insights

Addressing issues important to maintaining a reliable and resilient grid

ERCOT GRID SECURITY

ERCOT prepares year-round for any type of threat to the electric system. Whether the threat is cyber or physical, ERCOT invests in trained staff and resources to keep the electric grid safe. From system redundancies (backup systems) to controlled access, ERCOT employs multiple layers of protective measures to safeguard its critical infrastructure. This layered approach to cyber- and physical security is known as a defense-in-depth strategy, meaning ERCOT uses multiple, overlapping safeguards so that the system remains protected even if one layer is challenged. ERCOT collaborates with Market Participants (companies that generate, move, buy, sell, or use wholesale electricity within the ERCOT Region), as well as federal and state agencies, to detect threats early and coordinate responses effectively.

CYBER SECURITY

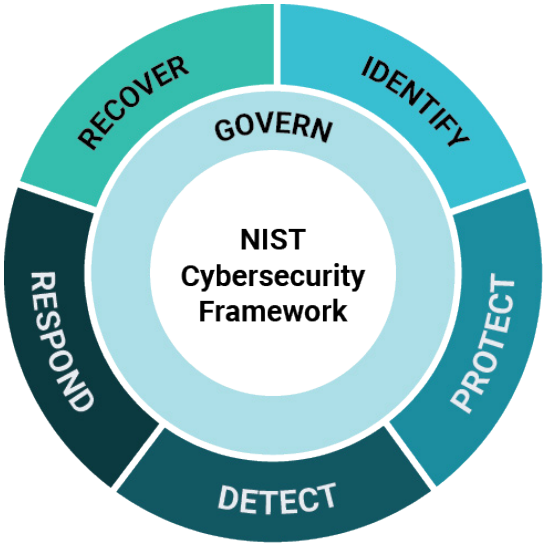
Overview: ERCOT is committed to protecting the electric system from cyber attacks that could compromise control of the grid. ERCOT complies with the federal Critical Infrastructure Protection (CIP) standards enforced by the North American Electric Reliability Corporation (NERC). Under these standards, ERCOT is required to address cyber risks and vulnerabilities by establishing controls to secure critical assets and their associated cyber systems. This includes reporting security incidents and maintaining recovery plans to be executed in the event of an emergency.

In addition to these federal requirements, Texas has enacted its own legislation to further strengthen cybersecurity oversight of the state's electric utilities.

In 2019, the Texas Legislature passed Senate Bill (SB) 936, which required the Public Utility Commission of Texas (PUCT) and ERCOT to contract with an entity to serve as the PUCT's cybersecurity monitor. The monitor manages a cybersecurity outreach program, communicating

emerging threats, reviewing cybersecurity self-assessments, researching and developing best business practices for cybersecurity, and reporting to the PUCT on cybersecurity preparedness for "monitored utilities" (ERCOT utilities and non-ERCOT utilities that opt into the program).

How it Works: In addition to the regulatory requirements identified above, ERCOT also follows the National Institute of Standards and Technology (NIST) Cybersecurity Framework when identifying and mitigating cyber threats. The NIST framework is a U.S. government-supported framework that consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The framework uses six functions to help ERCOT manage cybersecurity-related risk.



National Institute of Standards and Technology (NIST) Framework Elements

Why it Matters: As the operator of Texas' electric grid — one of the most vital infrastructures in the state — ERCOT's cybersecurity plan plays a critical role in protecting the 24/7 operation of the grid to keep power flowing to more than 27 million Texans.

TEXAS CYBER COMMAND (TXCC)

Overview: In 2025, the Texas Legislature passed House Bill (HB) 150, which created the Texas Cyber Command (TXCC) — a new state agency built to centralize and strengthen the state's cybersecurity defenses, particularly for its utilities and critical infrastructure vital for public health, safety, and economic development.

How it Works: The TXCC coordinates cybersecurity threat detection and response efforts across state, local, and federal agencies, ensuring a unified and coordinated approach when threats emerge. ERCOT is actively partnering with the TXCC to strengthen these efforts and ensure that Texas' electric grid remains a priority within the state's broader cybersecurity defense strategy.

Why it Matters: Cyber threats to critical infrastructure are growing in sophistication and frequency. The TXCC ensures that Texas is not relying solely on individual utilities to defend against these threats — instead, creating a coordinated, statewide line of defense that protects Texans' power supply and other essential services.

PHYSICAL INFRASTRUCTURE SECURITY

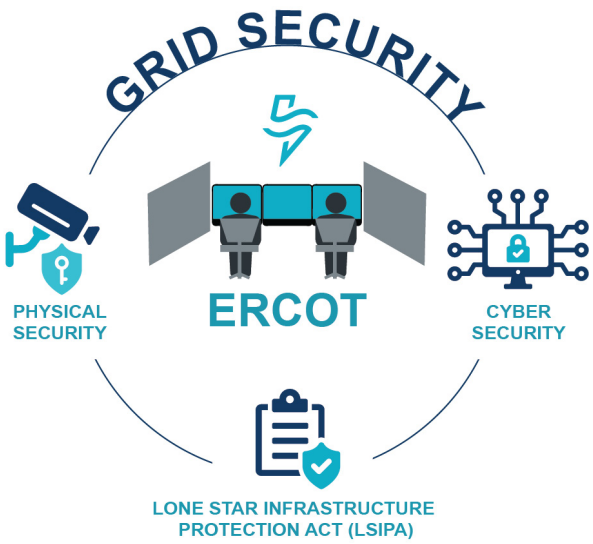
Overview: While ERCOT does not own or operate the generation and transmission facilities that supply power to the grid, it is critical that those facilities remain physically secure for ERCOT to reliably operate Texas' electric grid. ERCOT and the Market Participants operate their own control centers, which are built and reinforced to withstand physical threats and have back-up sites in the event that their primary control centers become inoperable.

How it Works: Market Participants are required under the NERC CIP standards and ERCOT Operating Guides to notify ERCOT of certain security incidents, such as vandalism or theft, that could compromise critical systems and impact grid reliability. Timely reporting is essential to ensure ERCOT can quickly support Market Participants in mitigating potential reliability risks to the grid. ERCOT and Market Participants undergo regular testing of their back-up control centers to ensure they are prepared if their primary facilities are unavailable.

Why it Matters: Physical security controls are critical given that much of Texas' electric grid infrastructure exists in public or open spaces. Quick, clear communication between ERCOT and the Market Participants on physical security threats or incidents ensures that ERCOT continues to operate a reliable grid.

LONE STAR INFRASTRUCTURE PROTECTION ACT (LSIPA)

Overview: The Lone Star Infrastructure Protection Act (LSIPA) enacted by the 87th Texas State Legislature in 2021, and amended by the Legislature in 2023 and 2025, is designed to protect Texas' critical infrastructure — like the ERCOT electric grid — from being accessed or controlled by companies linked to foreign countries including China, Russia, Iran, and North Korea.



ERCOT uses a layered approach to keep the electric grid secure.

How it Works: All companies operating within the ERCOT grid are required to comply with the LSIPA requirements and certify that they are in compliance with the Act's foreign ownership requirements. ERCOT applies these same requirements to vendors who contract to provide hardware, software, and other services to ERCOT. Any entity that cannot certify their compliance with the LSIPA criteria is prohibited from registering as a Market Participant or providing services to ERCOT.

Why it Matters: The Texas electric grid is a high-value target for 'bad actors,' and the LSIPA adds a critical line of defense against foreign interference, ensuring Texans' power supply remains secure and reliable.