Protecting ERCOT's electric system from cyber attacks

ERCOT prepares year-round for any type of threat to the electric system. Whether the threat is cyber or physical, ERCOT continually invests in trained staff and resources to keep the electric grid safe. ERCOT works closely with Market Participants (MPs) and government partners to detect threats early and coordinate responses. From system redundancies to controlled access, ERCOT employs multiple layers of protective measures to safeguard its critical infrastructure. This layered cyber- and physical security approach is known as a defense-in-depth strategy.

ERCOT complies with the federal critical infrastructure protection standards enforced by the North American Electric Reliability Corporation (NERC CIP), which require securing critical assets and cyber systems, reporting security incidents, and maintaining recovery plans. Texas legislation further strengthens these protections: the Lone Star Infrastructure Protection Act (LSIPA) guards the grid against foreign adversary access, and the Texas Cyber Command (TXCC), established in 2025, centralizes cybersecurity defense across the state's utilities and critical infrastructure. ERCOT actively partners with the Texas Cyber Command to strengthen its capabilities.

The ERCOT Critical Infrastructure Security Department uses industry best practices, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), to inform its cybersecurity policies and programs.

Security collaboration

ERCOT is committed to external collaboration with relevant government agencies, law enforcement, industry, and national labs to enhance its security presence. Federal and national agencies include the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Department of Energy (DOE), and many others. ERCOT also collaborates with the Electricity Information Sharing and Analysis Center (E-ISAC), Texas Cyber Command, and Texas Cybersecurity Council.

Additionally, ERCOT's **Critical Infrastructure Protection Working Group** meets routinely to discuss any security issues impacting the industry and ways to mitigate those risks.

Government Contact: **governmentrelations@ercot.com**
Media Contact: **media@ercot.com**

Grid Security Collaboration

Federal/National

- U.S. Department of Homeland Security
- Federal Bureau of Investigation
- Department of Energy
- Federal Energy Regulatory Commission
- Department of State
- Department of Justice
- United States Computer Emergency Readiness Team (US-CERT)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- National Electric Sector Cybersecurity Organization
- North American Electric Reliability Corporation
- Electricity Information Sharing & Analysis Center
- Multi-State Information Sharing & Analysis Center

State

- Public Utility Commission of Texas
- Texas Department of Public Safety
- Texas Department of Information Resources
- Texas Cybersecurity Council

Industry

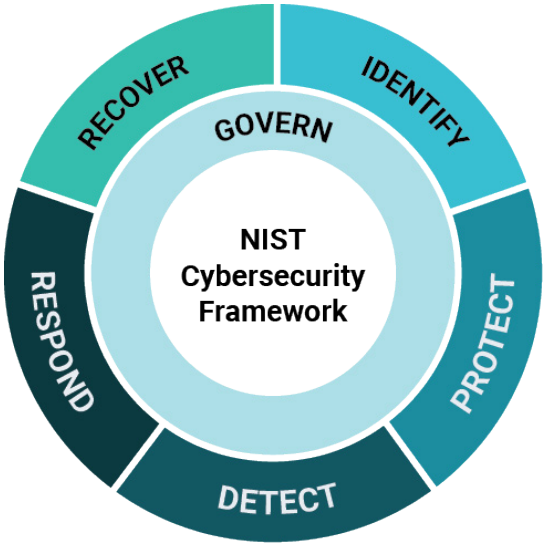
- North American Transmission Forum
- Electric Power Research Institute
- ISO/RTO Council

National Labs:

- Idaho National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories
- Argonne National Laboratory

Mitigating risk with the NIST Cybersecurity Framework

ERCOT aligns its cybersecurity practices with the NIST Cybersecurity Framework to identify and mitigate 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 organizations manage cybersecurity risk. Those functions are: Govern, Identify, Protect, Detect, Respond, and Recover.



Government Contact: governmentrelations@ercot.com
Media Contact: media@ercot.com