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 help keep the electric grid safe. From system redundancies to controlled access, ERCOT has 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.

The grid operator complies with the federal cybersecurity and critical infrastructure protection standards enforced by the North American Electric Reliability Corporation. These standards require bulk power system users, owners, and operators in the United States to address cyber risks and vulnerabilities by establishing controls to secure critical assets from physical and cyber sabotage, reporting security incidents and establishing plans for recovery in the event of an emergency.

The ERCOT Critical Infrastructure Security Department uses best industry practices, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), to help shape its own security 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) and Texas Cybersecurity Council.

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

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 and 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:

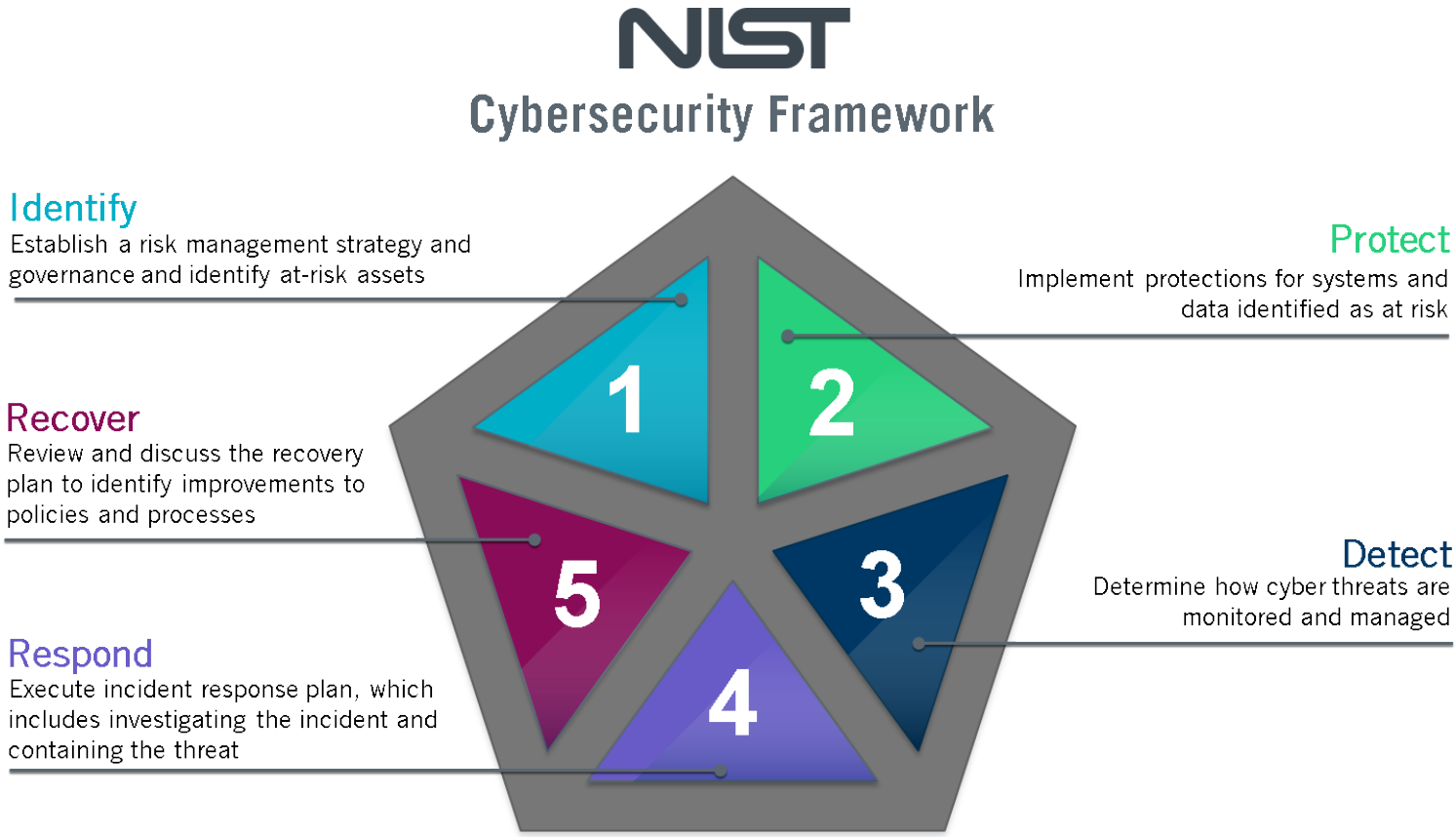
- Idaho National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories
- Argonne National Laboratory

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

March 2023

Mitigating risk with the NIST Cybersecurity Framework

ERCOT follows the 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 five functions to help owners and operators of critical infrastructure manage cybersecurity-related risk. Those functions are: Identify, Protect, Detect, Respond and Recover.



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

ercot
Your Power. Our Promise.