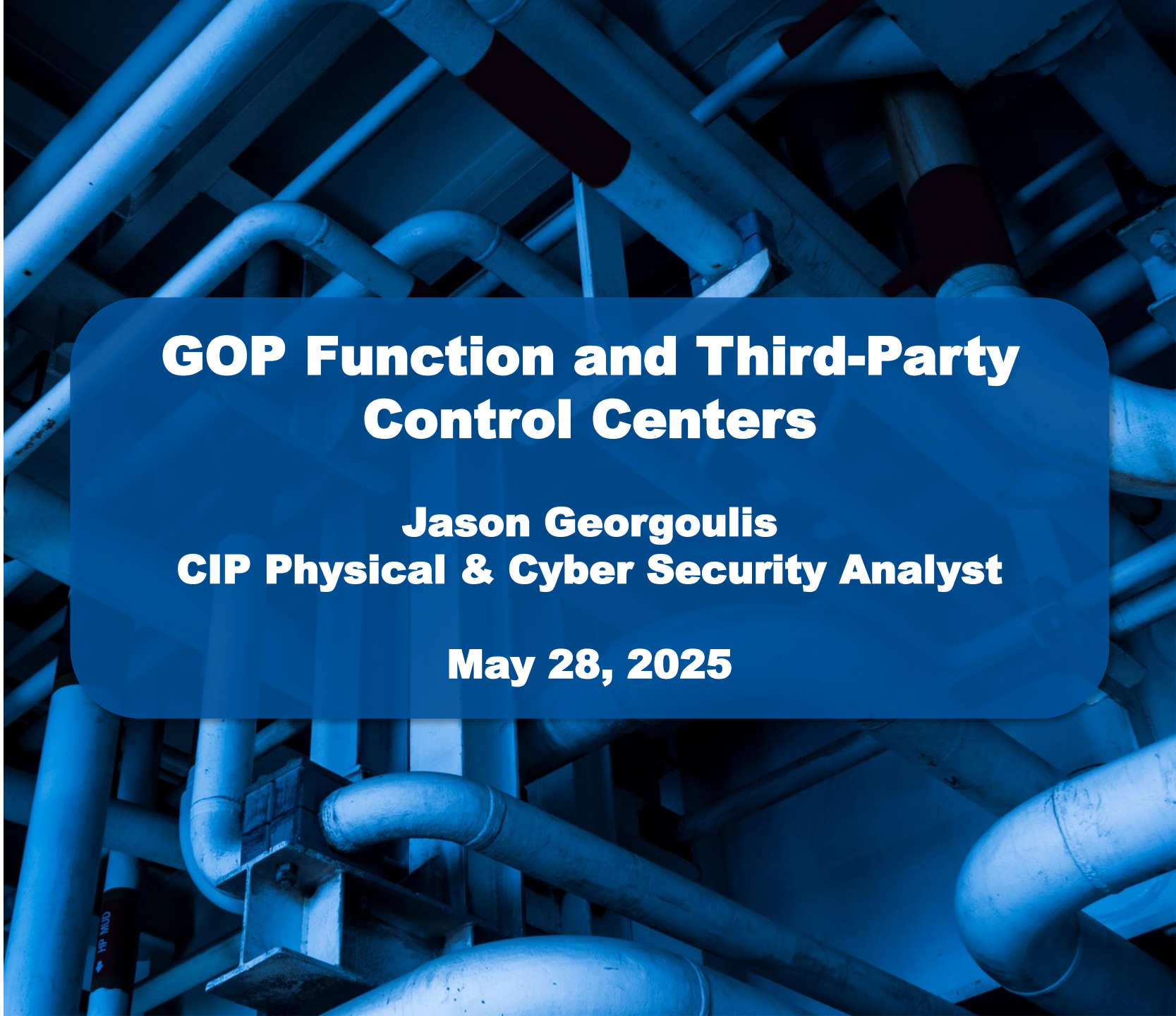
TEXAS RE

GOP Function and Third-Party Control Centers

Jason Georgoulis
CIP Physical & Cyber Security Analyst

May 28, 2025

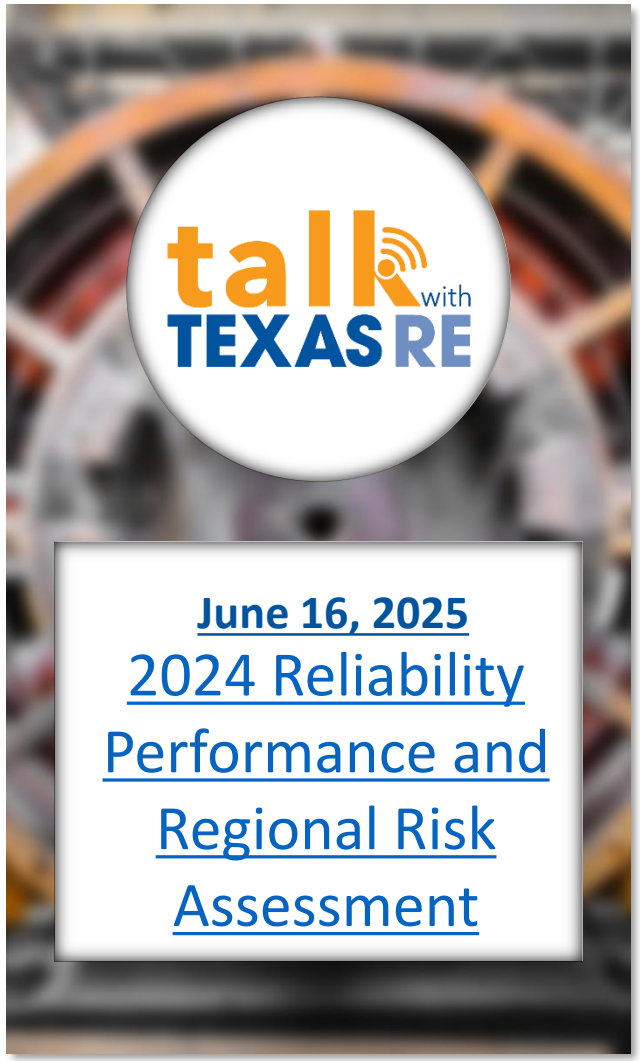


Antitrust Admonition

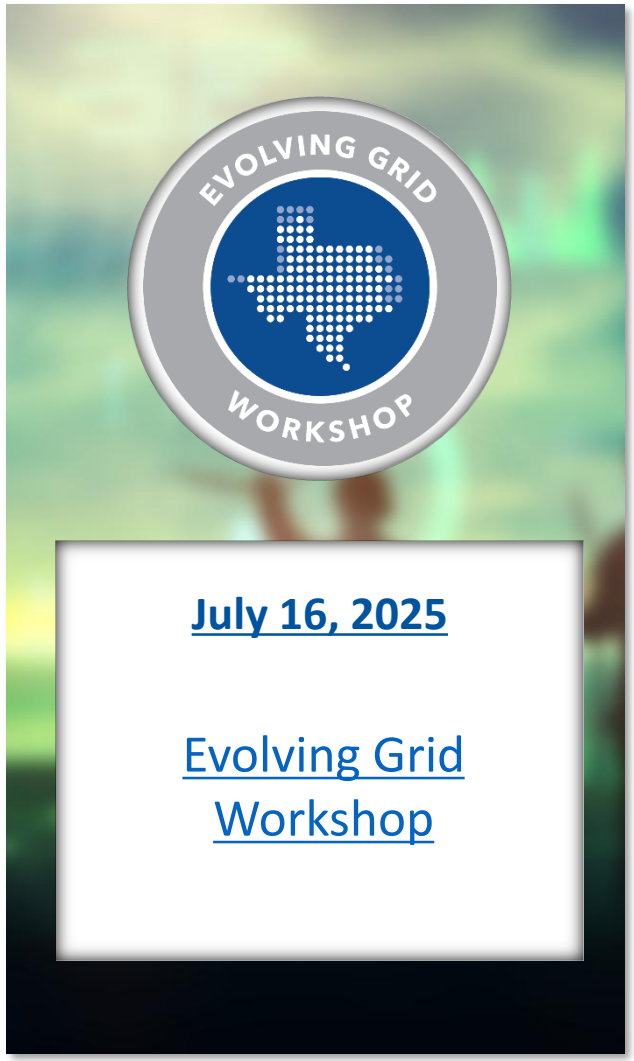
Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Upcoming Texas RE Events



Upcoming Texas RE Events



July 16, 2025

Evolving Grid Workshop

September 17, 2025

Q3 MRC, AGR&F, and Board Meetings

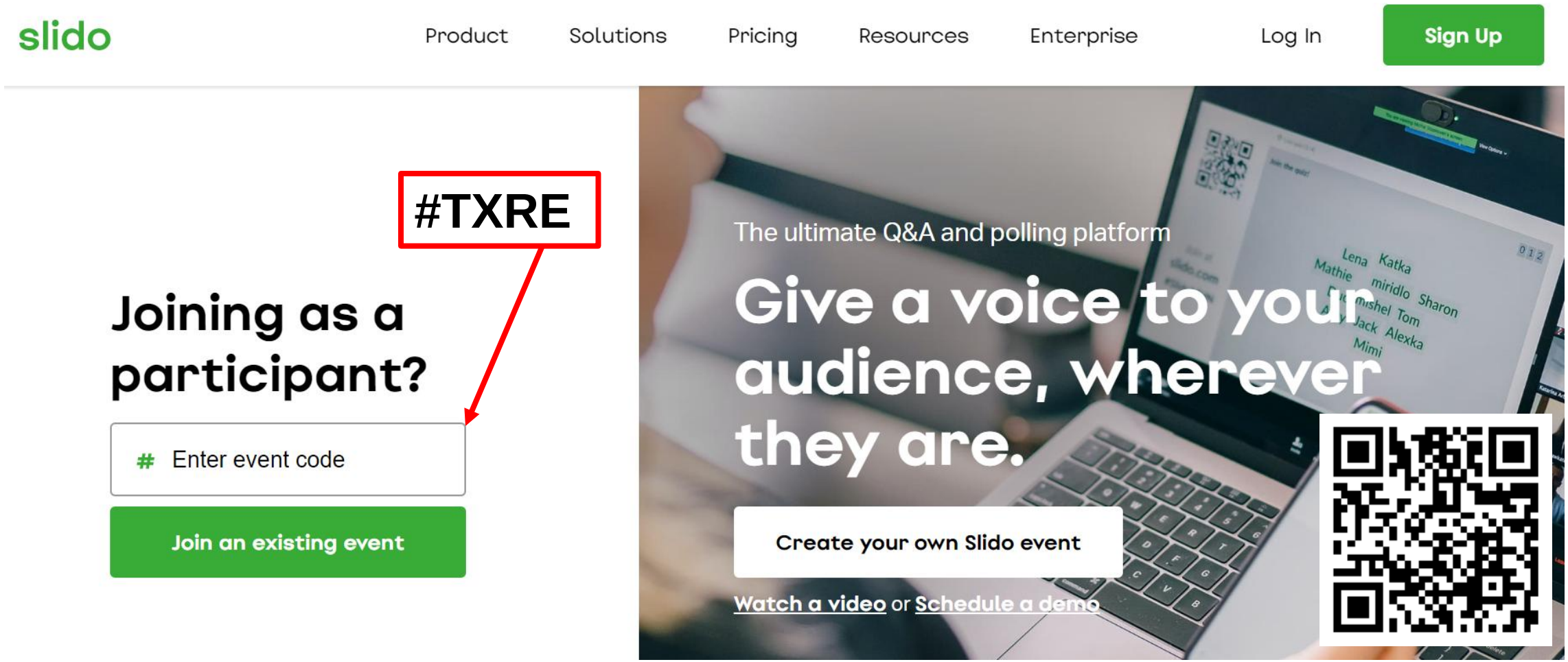
October 1, 2025

Winter Weatherization Workshop

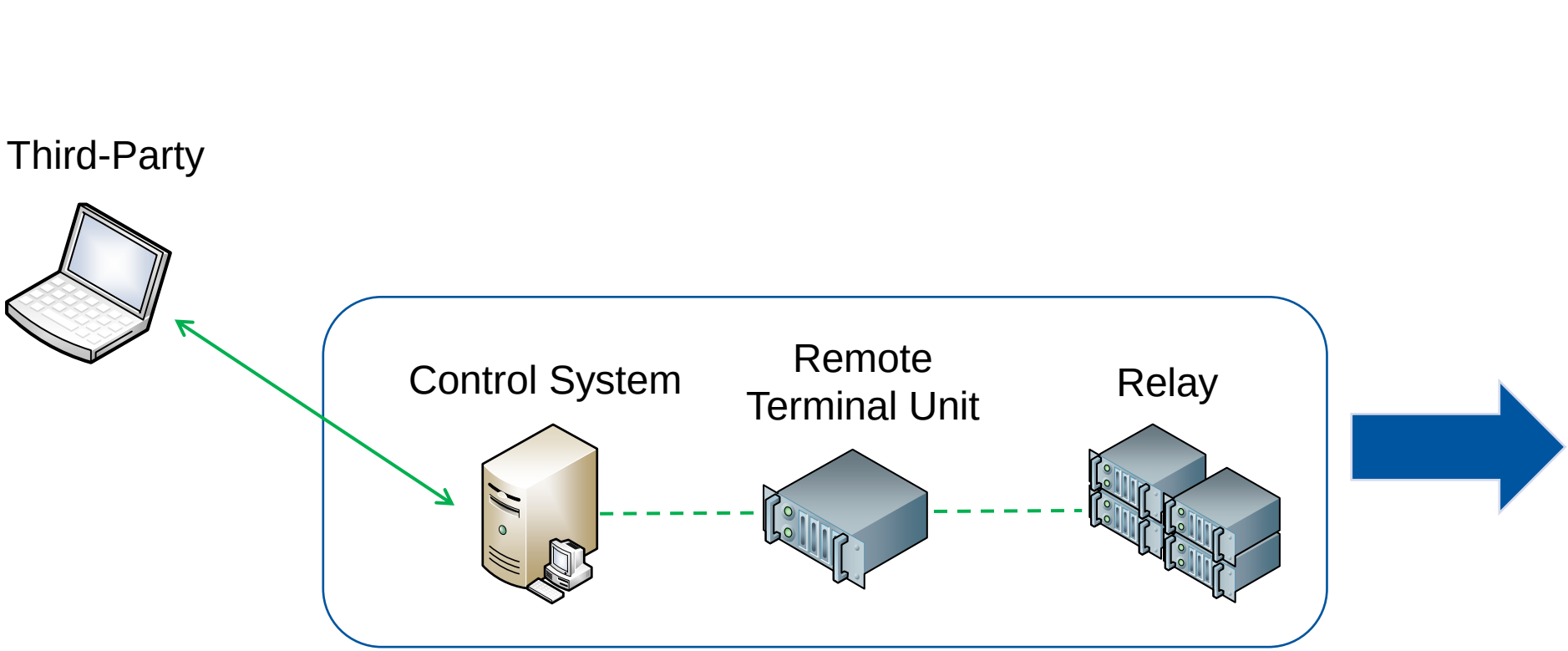
Upcoming ERO Enterprise Events

Date	Event
June 2	Summer Assessment Report & Summer Weather Review (SERC)
June 4	Reliability in the West: Large Load System Performance (WECC)
June 16	Technical Talk with RF (RF)
June 19	Reliability & Security Monthly Update (WECC)

Slido.com


slido
Product
Solutions
Pricing
Resources
Enterprise
Log In
Sign Up
#TXRE
Joining as a participant?
Enter event code
Join an existing event
The ultimate Q&A and polling platform
Give a voice to your audience, wherever they are.
Create your own Slido event
Watch a video or Schedule a demo

Third-Party Monitoring or Control

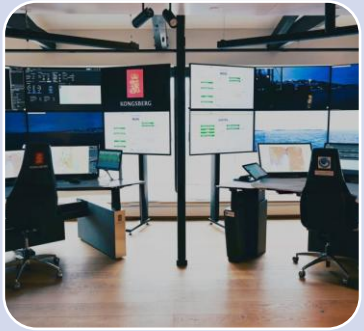


Agenda

Third-party device risks

Third-party connection risks

Low vs high risk when using a third-party



Remote Operation Centers (ROCs) risks

Recommended Controls to mitigate risks

Sli.do (#TXRE)

Slido Question

What operational risks would you consider if using a third-party to monitor or control generation?

Third-Party Vendor and Device Risks

Risks

- Unauthorized Access
- Exploitation of Device Vulnerabilities
- Introduction of Malware

Controls

- Background Checks/Offboarding
- Device Management Policies
- Cyber Hygiene Supply Chain Risk Management

Remote Connection Risks

Location of third-party?

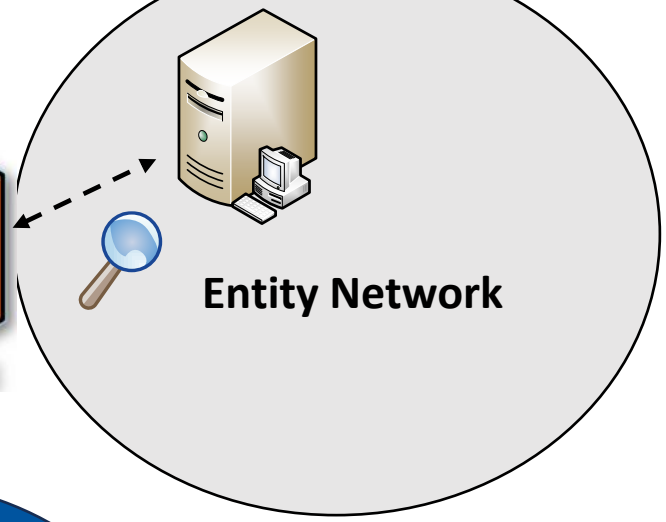
Malicious communications? Monitoring, logging, access control

Third-Party

Unauthorized disclosure? Encryption

Unauthorized access? MFA

Firewall



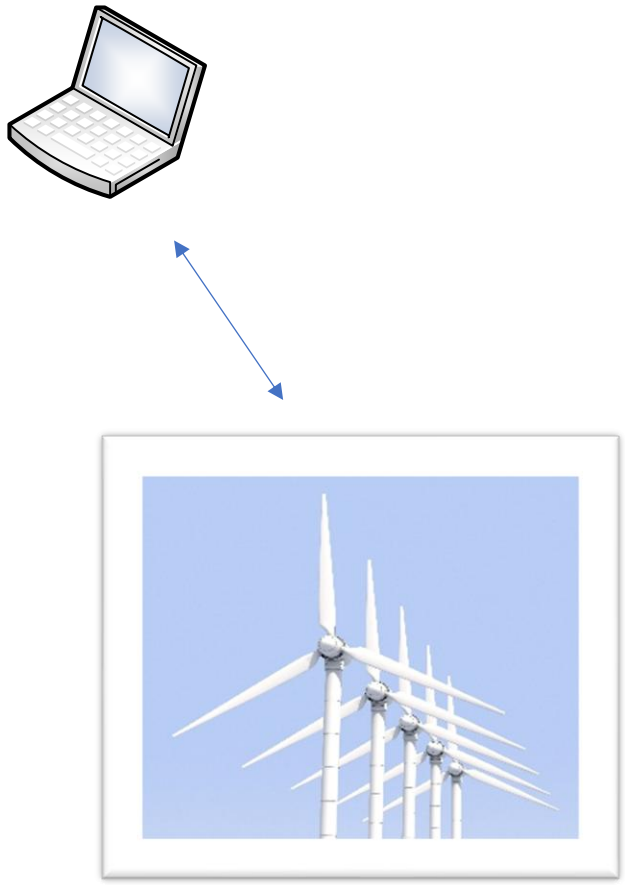
Entity Network

Privileged access?

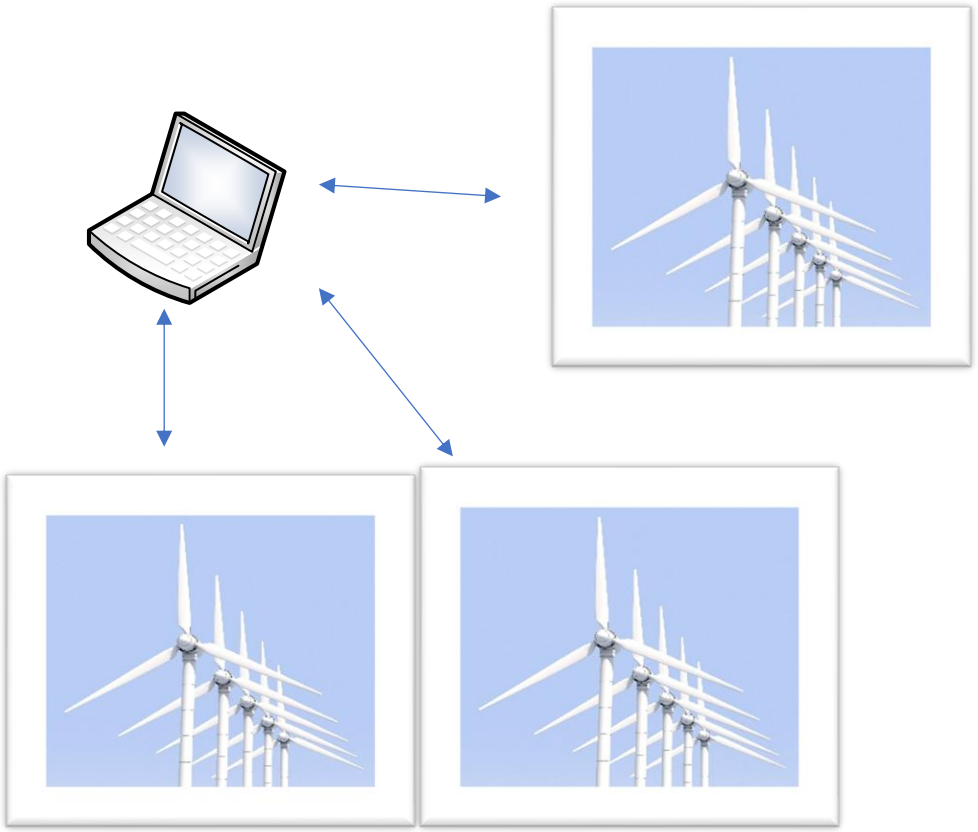
Persistent connection? No

Detective controls

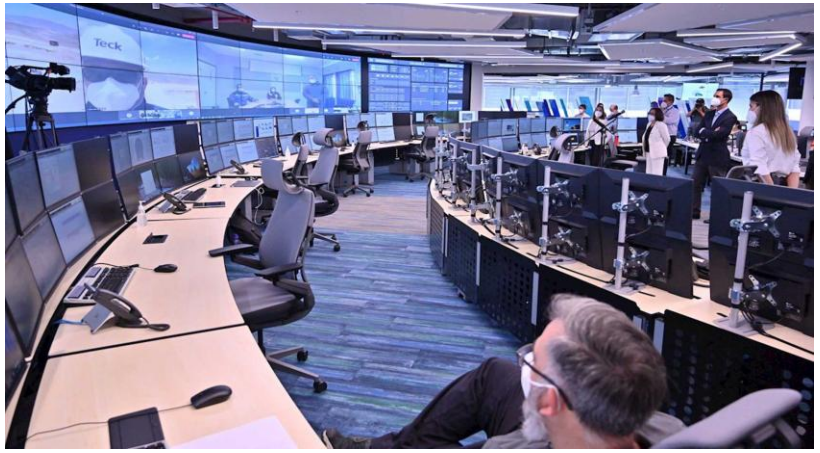
Low vs High Risk



Low or medium/high impact?



Remote Operation Center (ROC)



Are they controlling multiple low impact sites?

Recap Risks vs Controls

Risks

- Unauthorized disclosure
- Unauthorized access
- Introduction of malicious communications/code
- Lack of visibility

Controls

- Encryption
- Multi-factor authentication (MFA), strict access control lists, privileged access policies
- Intrusion detection/prevention systems, security information and event management, device management policies, deep pack inspection
- Methods to monitor and terminate sessions

Best Practices

- Understand what technology makes the facility work
- Understand the configuration
- Sufficient training and education

Resources

NERC

- ERO CMEP Implementation Plan v2.0 - 2025

RF

- 2024 CIP Themes and Lessons Learned

CISA

- 2023 Top Routinely Exploited Vulnerabilities | CISA
- Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA

NIST

- SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC
- Cryptographic Standards and Guidelines | CSRC

TEXAS RE
Ensuring electric reliability for Texans