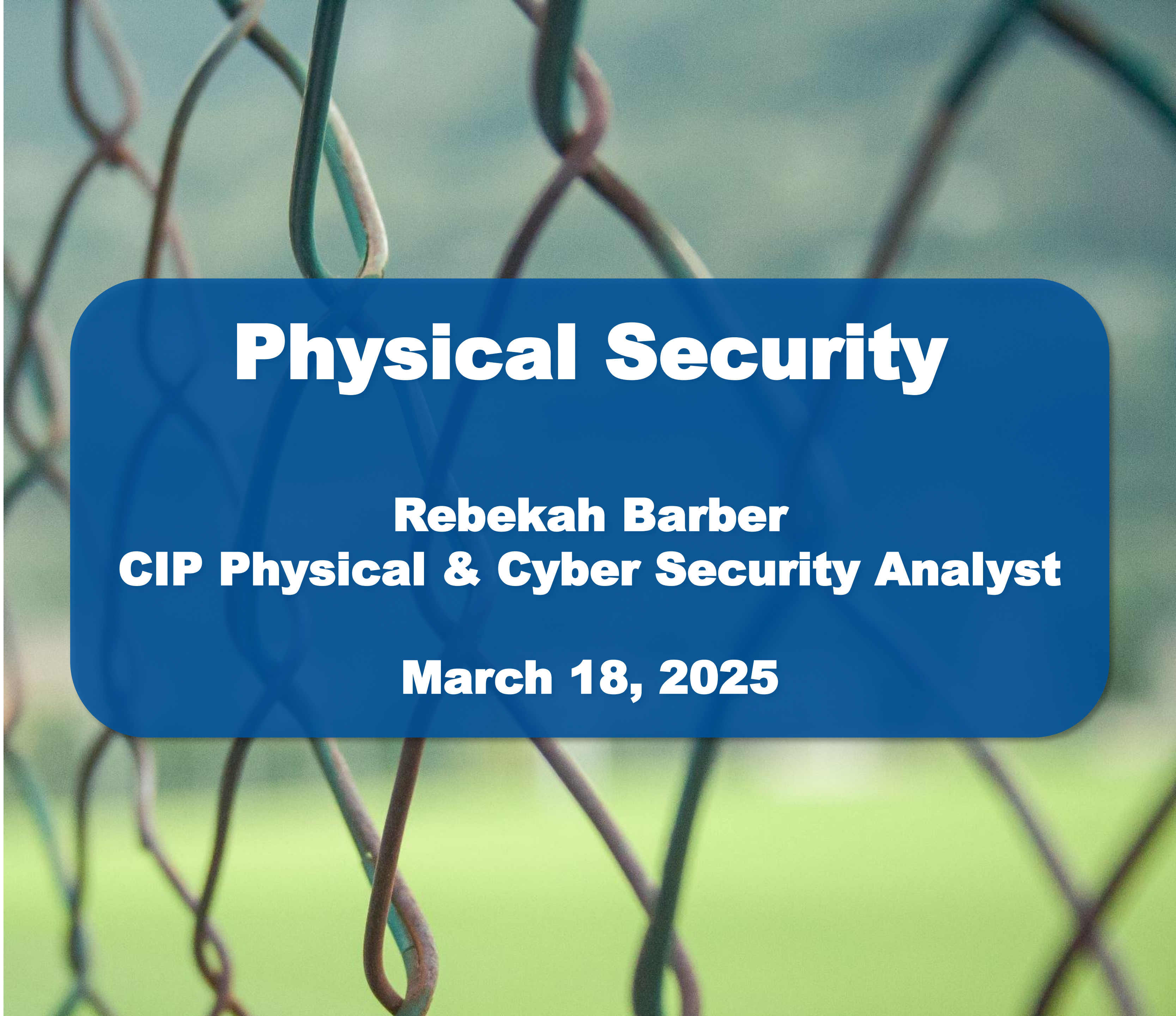
TEXAS RE



Physical Security

Rebekah Barber
CIP Physical & Cyber Security Analyst

March 18, 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.

talk with TEXAS RE

Upcoming Texas RE Events

talk with TEXAS RE

March 25, 2025

Training Exercises

talk with TEXAS RE

April 1, 2025

IBR Work Plans and Registration

talk with TEXAS RE

April 8, 2025

Trends for New Registrants

Upcoming Texas RE Events

April 23, 2025

Spring Standards, Security, & Reliability Workshop

May 14, 2025

Q2 MRC, AGR&F, and Board Meetings

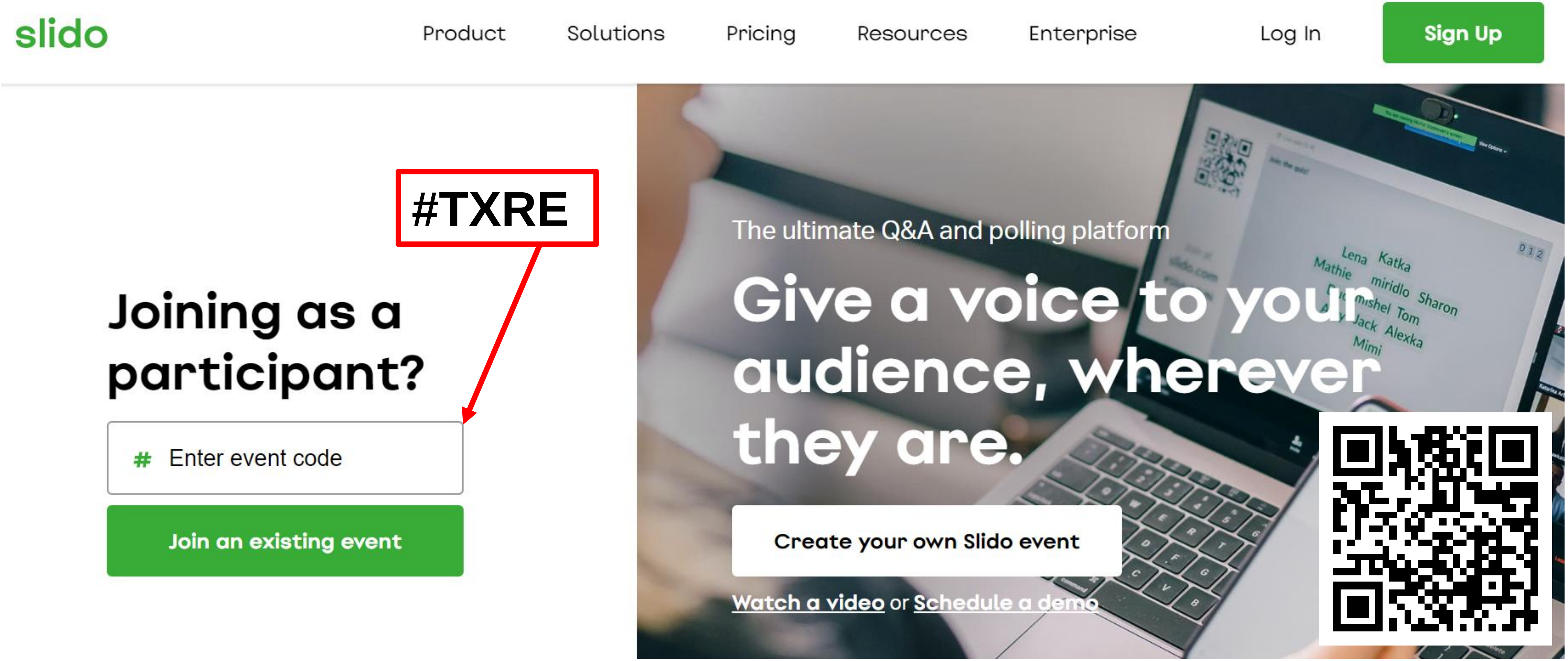
July 16, 2025

Evolving Grid Workshop

Upcoming ERO Enterprise Events

Date	Event
March 25-27	Physical Security Workshop (SERC)
March 25-27	Reliability & Security Workshop (WECC)
April 2	Application of IBR Practice Guide Workshop (SERC)
April 3	2025 Virtual RAM Conference (MRO)
April 8-10	System Operator Conference 1 (SERC)
April 10	GridEx VIII Preparation Webinar (MRO)

Slido.com



#TXRE

Joining as a participant?

The ultimate Q&A and polling platform

Give a voice to your audience, wherever they are.

Watch a video or Schedule a demo

2025 CMEP IP

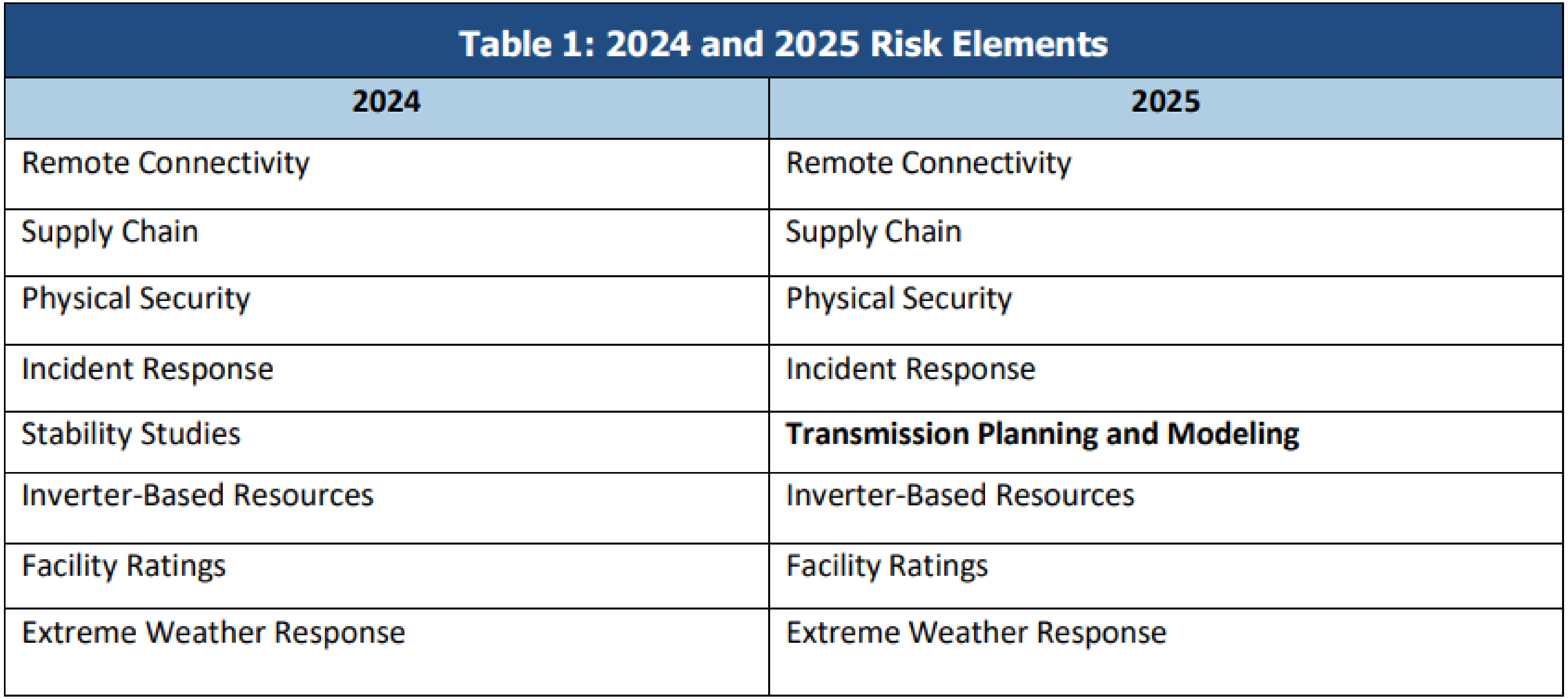


Table 1: 2024 and 2025 Risk Elements	
2024	**2025**
Remote Connectivity	Remote Connectivity
Supply Chain	Supply Chain
Physical Security	Physical Security
Incident Response	Incident Response
Stability Studies	**Transmission Planning and Modeling**
Inverter-Based Resources	Inverter-Based Resources
Facility Ratings	Facility Ratings
Extreme Weather Response	Extreme Weather Response

The Importance of Physical Security

Resilience and Continuity

Protection of BES Assets

Integration with Cybersecurity

Public Safety

Physical Security Process and the Standards

Assessment

(CIP-014-3)

Physical Protections

(CIP-003-8 and CIP-006-6)

Monitoring/Reporting

(CIP-006-6)

CIP-014-3 Assessment

R4. Each TO that identified a Transmission station, Transmission substation, or a primary control center in R1 and verified according to R2, and each TOP notified by a TO according to R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in R1 and verified according to R2.

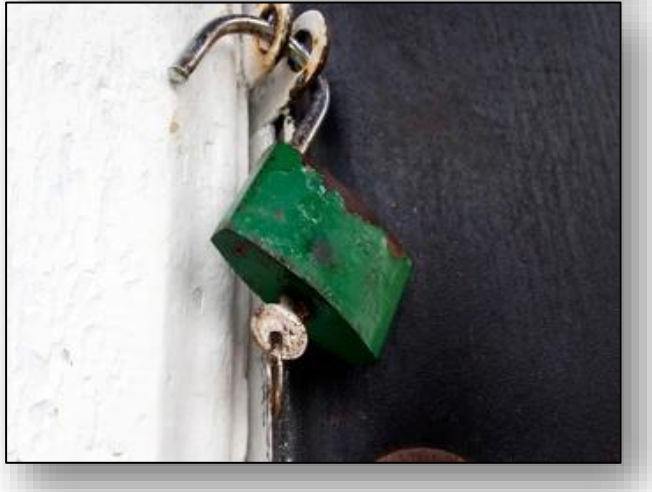
The evaluation shall consider the following:

Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary Control Center(s);

Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events

Intelligence or threat warnings received from sources such as law enforcement, the ERO, the E-ISAC, U.S. federal and/or Canadian governmental agencies, or their successors

CIP-003-8 Physical Protections



Section 2: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to:

- The asset or the locations of the low impact BES Cyber Systems within the asset
- The Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any

CIP-006-6 Key Definitions

Physical Security Perimeter (PSP)

- The physical, completely enclosed “six-wall” border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled

Physical Access Control System (PACS)

- Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers

NERC Glossary of Terms

CIP-006-6 Physical Protections

Only Medium Impact BCS with ERC

<u>Part 1.2</u> Utilize at least one physical access control to allow only individuals who have authorized unescorted physical access into the Physical Security Perimeter (PSP)

Only High Impact BCS

<u>Part 1.3</u> Utilize at least two or more different physical access controls

<u>Part 1.10</u> Restrict physical access to cabling and nonprogrammable communication components outside of the PSP or encrypt/monitor the status of the link and issue an alarm or alert within 15 minutes of detection, or equal logical protection

<u>Part 2.1</u> Require continuous escorted access of visitors within each PSP, except during CIP Exceptional Circumstances

<u>Part 3.1</u> Maintenance and testing of each Physical Access Control System (PACS) and locally mounted hardware or devices at the PSP at least once every 24 calendar months to ensure they function properly

CIP-006-6 Monitoring and Reporting

Part 1.4 Monitor for unauthorized access into a PSP

Part 1.5 Issue an alarm or alert in response to detected unauthorized access through a physical access point to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection

Part 1.6 Monitor each PACS for unauthorized physical access

Part 1.7 Issue an alarm or alert of detected unauthorized physical access of a PACS to personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection

Part 1.8 Log entry of everyone with authorized unescorted physical access into each PSP

Part 1.9 Retain physical access logs for at least 90 days

Part 2.2 Require manual or automated visitor logging

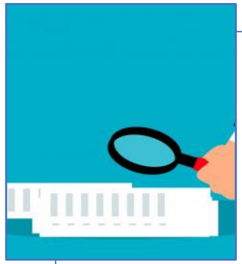
Part 2.3 Retain visitor logs for at least 90 days

Walkthroughs During an Audit

Inspect the perimeter to ensure it is adequate to deter unauthorized access

Test access control measures to ensure only authorized individuals can enter secure areas

Review environmental controls for Controls Centers and associated datacenters



Review visitor logs to ensure continuous escorted access of visitors within the PSP

Check surveillance and monitoring systems to verify functionality and coverage

Best Practices

- Avoid Single Points of Failure
- Actively Monitor PACS Health
- Avoid Alarm Fatigue
- Coordinate with Local Law Enforcement
- Employee Training

Questions?

TEXAS RE

Ensuring electric reliability for Texans