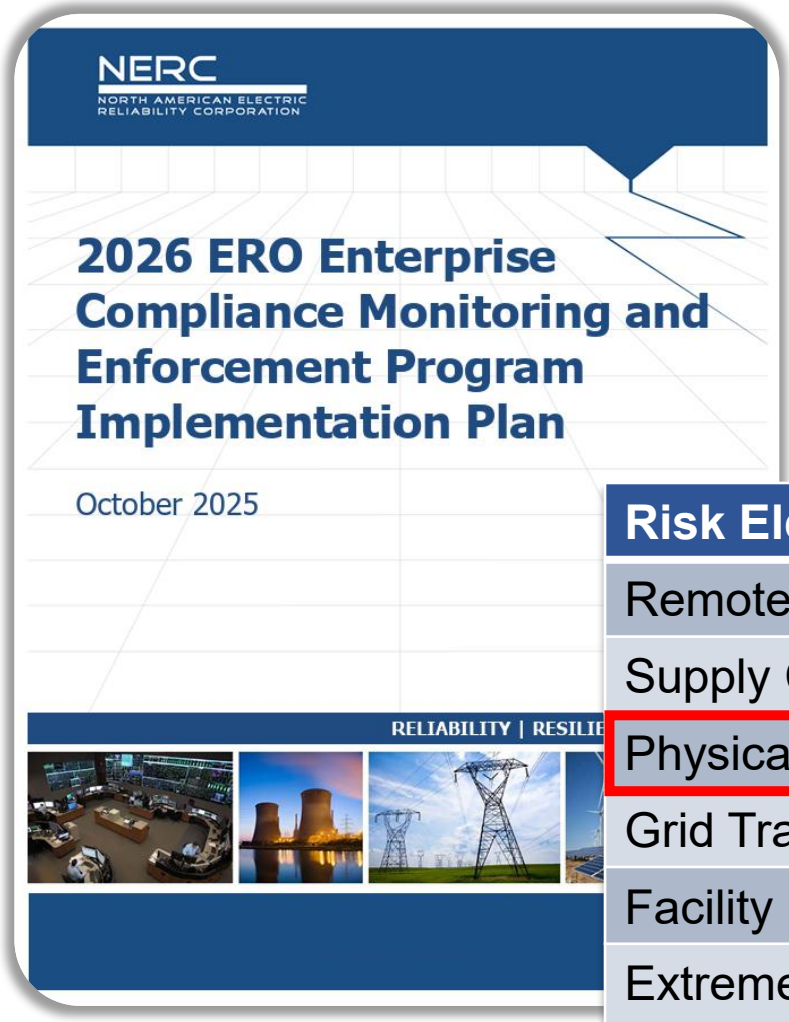
TEXAS RE

2026 CMEP IP Risk Element - Physical Security CIP-014-3 R4 R5

Chris Mejia
CIP Cyber & Physical Security Analyst

May 1, 2026

Risk Focus & CMEP IP Risk Factors



Risk Elements
Remote Connectivity
Supply Chain
Physical Security
Grid Transformation
Facility Ratings
Extreme Weather Response

CIP-014-3 R4 – Physical Security

- **R4.** Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement 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 Requirement R1 and verified according to Requirement R2.

4.1 Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s)

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

4.3 Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO) Enterprise, the Electricity Information Sharing and Analysis Center (E-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors

CIP-014-3 R4 – Physical Security

Best Practices

Leverage public resources (i.e., CISA.gov, NERC Security Guideline)

CIP-014-3 R5 – Physical Security

- **R5.** Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s).

5.1 Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4

5.2 Law enforcement contact and coordination information

5.3 A timeline for executing the physical security enhancements and modifications specified in the physical security plan

5.4 Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s)

CIP-014-3 R5 – Physical Security

Best Practices

- Consider testing security controls
- Familiarization with local law enforcement
- Calendar reminders, notification system
- Leverage public resources (i.e., CISA.gov, NERC Security Guideline)

Questions?

TEXAS RE
Ensuring electric reliability for Texans