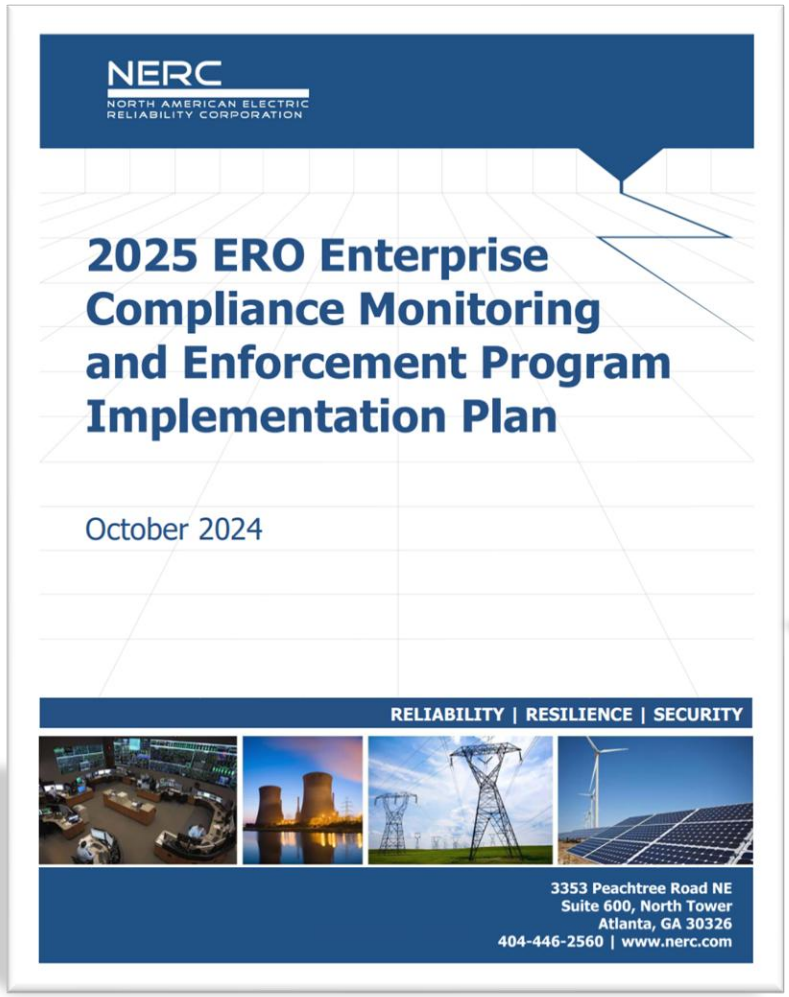
TEXAS RE

CIP-014-3 R4, R5

Paul Hopson
CIP Compliance Team Lead

May 9, 2025

2025 ERO CMEP IP – Physical Security



Physical Security

Physical security threats continue to be a top concern in 2025 as threat levels have remained elevated. An area of particular focus should be opportunistic domestic violent extremists. They aim to exploit potential social unrest such as political elections, economic issues, and activistic causes to target infrastructure.[13] More than ever, there are more entities with assets that contain low impact BES Cyber Systems being registered across the ERO. There needs to be a concerted effort around these assets that contain low impact BES Cyber Systems as there has been an upward trend in violations regarding physical security plans, electronic security perimeters, and access management and revocation to name a few.[14] One of the many challenges of executing a physical security program is managing tasks that require repetitive behavior over significant periods of time, as there is increased potential for personnel to lose focus on the performance of an individual act or forget the importance of the act itself. Examples of this behavior that has been observed would be that in multiple instances, an employee who was running late to a shift, without their badge, was able to talk their way through multiple barriers and into a Physical Security Perimeter (PSP).[15] This theme highlights examples of apathy, circumvention, complacency, inattentiveness, and other types of "performance drift" in physical security programs at entities of every size and type.[16]

Risk Element Areas of Focus: Physical Security

CIP-014-3: Physical Security

Rationale	Standard	Req	Entities for Attention
Mitigate risks to the reliable operation of the BES as the result of a Physical Security Incident.	CIP-014-3	R4, R5	Transmission Operator Transmission Owner

CIP-014-3

- 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. The evaluation shall consider the following:
  - **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; and
  - **4.3.** Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

CIP-014-3

- 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). The physical security plan(s) shall include the following attributes: 4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(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 Best Practices and Considerations

R4

- *Assess the potential threats of physical attacks on each transmission station, substation, and primary Control Center identified in R1 and verified in R2.*
- *The entity must analyze the 'who,' 'what,' 'where,' 'how,' and 'how many' regarding potential physical attacks:*
  - *What is the mission of the potential attackers?*
  - *How determined are they to achieve their mission?*
  - *How many individuals may be involved in the attack?*
  - *What tools or weapons might they possess?*
  - *What vehicles or machinery could they utilize? (This may include a line truck or other equipment available on-site).*
  - *How might this individual or group execute a physical attack?*
- *Conduct a thorough evaluation of the potential threats posed by physical attacks on each transmission station, substation, and primary Control Center identified in R1 and verified in R2.*
- *If the primary first responders are not law enforcement, what is the estimated response time and personnel strength upon their arrival?*
- *What level of authority does law enforcement have to act on entity property?*

R5

- *Base the security plan on the comprehensive list of prioritized threats and vulnerabilities identified in R4.*
- *Ensure that the chosen security solutions are suitable for mitigating the identified threats or vulnerabilities.*
- *Include a matrix, narrative, or both in the security plan that accurately describes the solution's effectiveness based on specific attack scenarios (e.g., what to deter, detect, delay, and assess).*
- *Document unmitigated risks in the security plan, providing a rationale for any legal or technological limitations, and include a process for future state mitigation as solutions become available (e.g., UAVs or drones).*
- *Ensure that the process for assessing, communicating, and responding encompasses activities before, during, and after a physical attack.*
- *Develop the program to enhance the safety, familiarity, response time, and capability of first responders for potential physical attack scenarios.*
- *It is recommended that entities establish a clear mapping between the protections implemented in part R5 and the threats and vulnerabilities identified in part R4 within the security plan. Documenting this mapping is vital to ensure there are no gaps in protection and that the implemented measures effectively address the identified threats and vulnerabilities. Furthermore, this mapping serves as concrete evidence for third-party reviews, demonstrating that the threats and vulnerabilities are being adequately managed.*

CIP-014-3 Resources

- CMEP Practice Guide CIP-014-2
- CIP-014-2 R4 Evaluating Potential Physical Security Attack.pdf
- NERC Reliability Standard CIP-014-1 Requirement 5 Practices Guide
- NERC Project 2023-06 CIP-014 Risk Assessment Refinement

TEXAS RE
Ensuring electric reliability for Texans