

PHYSICAL & ELECTRONIC SECURITY GAP ASSESSMENT

Critical Infrastructure Perimeter / Access Corridor

Framework: CPTED • NERC CIP-014 • Critical Infrastructure Protection Best Practices



Prepared: Aug 1, 2026 – By Msc. Pedro Barrueco Perez
Based on visual/photographic review and publicly available security standards

Disclaimer: This assessment is based exclusively on a single photograph and is provided strictly for educational purposes. In practice, every organization tailors its security investments according to its unique risk profile and aligns its designs not only with established parameters and industry standards, but also with its own bespoke, proprietary security frameworks. Because security is inherently context-dependent and multi-layered, my observations constitute just one potential viewpoint—and should never be mistaken for a definitive, exhaustive, or universally applicable solution.

1. Executive Summary

The photograph shows a fenced, mesh-screened access corridor terminating at a gated entry to what appears to be an electrical substation or comparable critical infrastructure facility. A single street-light luminaire, chain-link fencing with barbed-wire outriggers, privacy mesh, and a small warning placard are visible. No cameras, intrusion detection, vehicle barriers, or reinforced signage are visible in the frame.

Applying Crime Prevention Through Environmental Design (CPTED) principles and the NERC CIP-014 physical security standard for Bulk Electric System (BES) facilities, this site shows gaps across nearly every control layer: surveillance, detection, delay, deterrence, and response. Because the asset class (electrical substation infrastructure) falls into the category NERC CIP-014 was written to protect, following the 2013 Metcalf sniper attack, the gaps below are evaluated against both a general CPTED lens and the specific intent of CIP-014, plus additional critical-infrastructure-specific considerations that go beyond either framework.

Overall current-state rating: WEAK. Baseline deterrence (fencing, barbed wire, some lighting) is present, but detection, verification, delay-in-depth, and response capability are effectively absent from what is visible.

2. CPTED Gap Analysis

CPTED rests on four reinforcing principles: Natural Surveillance, Natural Access Control, Territorial Reinforcement, and Maintenance. Each is assessed below against the observed conditions.

CPTED Principle	Observed Condition	Identified Gap	Recommendation
Natural Surveillance	Privacy mesh blocks sightlines in both directions; single light fixture creates high-contrast shadow zones near the gate and far fence line.	No informal “eyes on the corridor” from outside; blind approach to the gate; light/dark contrast aids concealment rather than deterring it.	Add secondary/motion-activated lighting at the gate; consider mirrors at blind corners; evaluate mesh height/placement vs. sightline needs.
Natural Access Control	Single vehicle/pedestrian gate secured with what appears to be a manual chain/padlock; no visible card reader, keypad, or intercom.	No audit trail of entries/exits; no way to verify identity remotely before granting access; single point of failure if lock is defeated.	Upgrade to electronic access control (card/PIN/biometric) with logging; add an intercom/video call point for identity verification.
Territorial Reinforcement	Only small placards mounted on the gate itself; no perimeter-length signage.	Insufficient signaling of ownership, monitoring, and consequences along the full fence run; reduces psychological deterrence for casual trespass.	Install larger, evenly spaced signage along the entire perimeter: no trespassing, video surveillance in use, electrical hazard, and owner/operator identification.
Maintenance (“Image & Milieu”)	Cracked and patched concrete/asphalt pavement visible in the foreground.	Visible deferred maintenance is a classic broken-windows signal that can lower perceived guardianship and invite testing of defenses.	Repair pavement and maintain visible upkeep as part of routine site management; treat visible condition as a security signal, not only a safety one.

3. NERC CIP-014 Gap Analysis

NERC CIP-014 (“Physical Security”) applies to Transmission Owners with stations, substations, and primary control centers whose loss could cause instability, uncontrolled separation, or cascading failure of the Bulk Electric System. It was developed in direct response to the 2013 Metcalf substation attack, and its core requirements (R1–R6) move from risk assessment through to a documented, third-party-reviewed physical security plan. The table below maps what is visible in the photo against the intent of the standard's operative requirements, it is not a compliance determination, since that requires the full risk assessment and non-public plan documentation.

CIP-014 Element	Standard's Intent	Observed Gap (from photo)	Recommendation
R1–R3: Risk Assessment & Verification	Identify critical stations/substations and have the assessment independently verified.	Not visible/determinable from a photo — but the absence of any hardened controls suggests the site may not yet reflect a completed risk-driven security plan.	Confirm whether this facility has undergone a CIP-014 risk assessment and, if applicable, third-party verification.
R4–R5: Physical Security Plan – Detection	Plans should include intrusion detection: fence sensors, video analytics, sound/gunshot detection.	No visible cameras, fence-mounted sensors, or acoustic/gunshot detection equipment.	Deploy CCTV with video analytics at the gate and along vulnerable fence spans; add fence-mounted vibration/strain sensors; evaluate acoustic gunshot detection given CIP-014's origin in a sniper attack.
R4–R5: Physical Security Plan – Delay (“Protection in Depth”)	Multiple layers of delay between the perimeter and critical equipment (buffer zones, secondary fencing, hardened barriers).	Only a single fence line and gate are visible; no buffer zone or secondary delay layer apparent between the corridor and the equipment yard beyond.	Introduce a buffer zone concept along the outer fence; consider a secondary interior barrier around the most critical equipment (transformers).
R4–R5: Vehicle/Ballistic Considerations	Post-Metcalf guidance emphasizes standoff distance, ballistic/vehicle barriers around critical equipment.	No bollards, K-rated barriers, or ballistic screening visible at the gate or along sightlines into the equipment yard.	Add vehicle barriers (bollards or crash-rated gate) at the entrance; evaluate ballistic screening/berms for line-of-sight protection of critical transformers.
R5: Law Enforcement Coordination	Physical security plans must document coordination with law enforcement for response.	Not determinable from photo; no visible signage referencing a monitored/patrolled status.	Confirm a documented law-enforcement liaison and response protocol exists and is exercised/tested periodically.
R6: Third-Party Plan Review	An unaffiliated third party must review the physical security plan periodically.	Not determinable from photo.	Verify the review cadence and most recent review date as part of a documentation audit (separate from this visual assessment).

4. Additional Considerations for Critical Infrastructure

Beyond CPTED and CIP-014's baseline requirements, critical infrastructure sites (substations, generation facilities, water/telecom nodes) increasingly need to account for threats and controls that neither framework spells out in full. These are worth evaluating even where CIP-014 does not strictly apply or has already been satisfied on paper:

- **Unmanned Aircraft System (UAS/drone) detection** — aerial surveillance and drone-delivered threats are a growing concern for substations and are not addressed by fencing or ground-level sensors at all.
- **Standoff distance and ballistic hardening** — sightline and berm/wall protection for the most critical equipment (transformers, breakers), directly responsive to the Metcalf attack method.
- **Redundant power and communications for security systems themselves** — cameras, sensors, and access control that fail when site power fails create a predictable attack window.
- **Cyber-physical convergence** — physical access to a substation often provides a path to SCADA/ICS equipment; physical security plans should be coordinated with the separate NERC CIP cyber security standards (CIP-005, CIP-007) rather than treated in isolation.
- **Insider threat / personnel vetting** — background checks, escort procedures for contractors, and access logging for authorized personnel, not just outsider intrusion.
- **Seismic/vibration and thermal (infrared) sensing** — useful in unmanned sites to detect both intrusion and equipment failure/fire risk simultaneously.
- **Tested incident response and law-enforcement notification protocol** — a documented plan is only as good as its last tabletop exercise or live test.
- **Environmental design against tools/vehicles being pre-staged nearby** — CPTED's "target hardening" extends to restricting concealment/staging areas immediately outside the fence line, not just inside it.
- **Redundant/backup lighting circuits** — a single luminaire, as observed, is also a single point of failure for the one passive deterrent currently in place.

5. Security Posture Scoring Matrix

A simplified 1–5 scale (1 = absent/critical gap, 5 = fully mature) based solely on what is visible in the photograph. This is illustrative, not a certified audit score.

Control Category	Current (Observed)	Target	Notes
Perimeter Fencing / Barbed Wire	3	4–5	Present but no anti-climb base treatment or vehicle barriers visible.
Lighting	2	4–5	Single fixture; no redundancy; strong shadow zones at gate.
CCTV / Video Analytics	1	4–5	None visible.
Intrusion Detection (fence/ground sensors)	1	4	None visible.

Control Category	Current (Observed)	Target	Notes
Access Control (gate)	1	4	Appears to be manual lock only.
Signage / Territorial Reinforcement	2	4	Small placards only, gate-mounted.
Vehicle / Ballistic Barriers	1	3–4	None visible; relevant given CIP-014 origin.
Natural Surveillance	2	3–4	Mesh screening blocks sightlines both directions.
Site Maintenance / Image	3	4	Cracked pavement; otherwise tidy.

6. Prioritized Recommendations

1. Immediate (0–3 months)

- Add motion-activated supplemental lighting at the gate to remove shadow zones.
- Install visible CCTV (even a single wide-angle camera with recording) covering the gate and corridor.
- Add perimeter-length warning/deterrent signage, not just gate placards.

2. Short-term (3–12 months)

- Upgrade gate lock to an auditable electronic access control system with remote verification (intercom/video call point).
- Install fence-mounted intrusion detection (vibration/strain or fiber-optic sensing).
- Repair pavement and address other visible deferred-maintenance items.

3. Medium/Long-term (12+ months)

- Evaluate and install vehicle barriers (bollards or a crash-rated gate) consistent with CIP-014 post-Metcalf guidance.
- Assess line-of-sight/ballistic exposure of critical equipment and consider screening or berms.
- Confirm and, if needed, initiate a formal CIP-014 risk assessment (R1–R3) if this facility meets applicability thresholds, including third-party verification (R2) and plan review (R6).
- Evaluate UAS/drone detection and cyber-physical (SCADA) coordination with the site's broader NERC CIP program.

7. Limitations of This Assessment

This assessment is based on a single photograph and publicly available security literature (CPTED principles and the published NERC CIP-014 standard and related guidance). It does not reflect confirmed knowledge of the facility's ownership, criticality classification, existing (non-visible) security controls such as buried sensors or off-frame cameras, or any completed risk assessment. It should be treated as a discussion starting point, not a substitute for a licensed physical security consultant's on-site survey or a Transmission Owner's own CIP-014 compliance process.