TEXAS RE

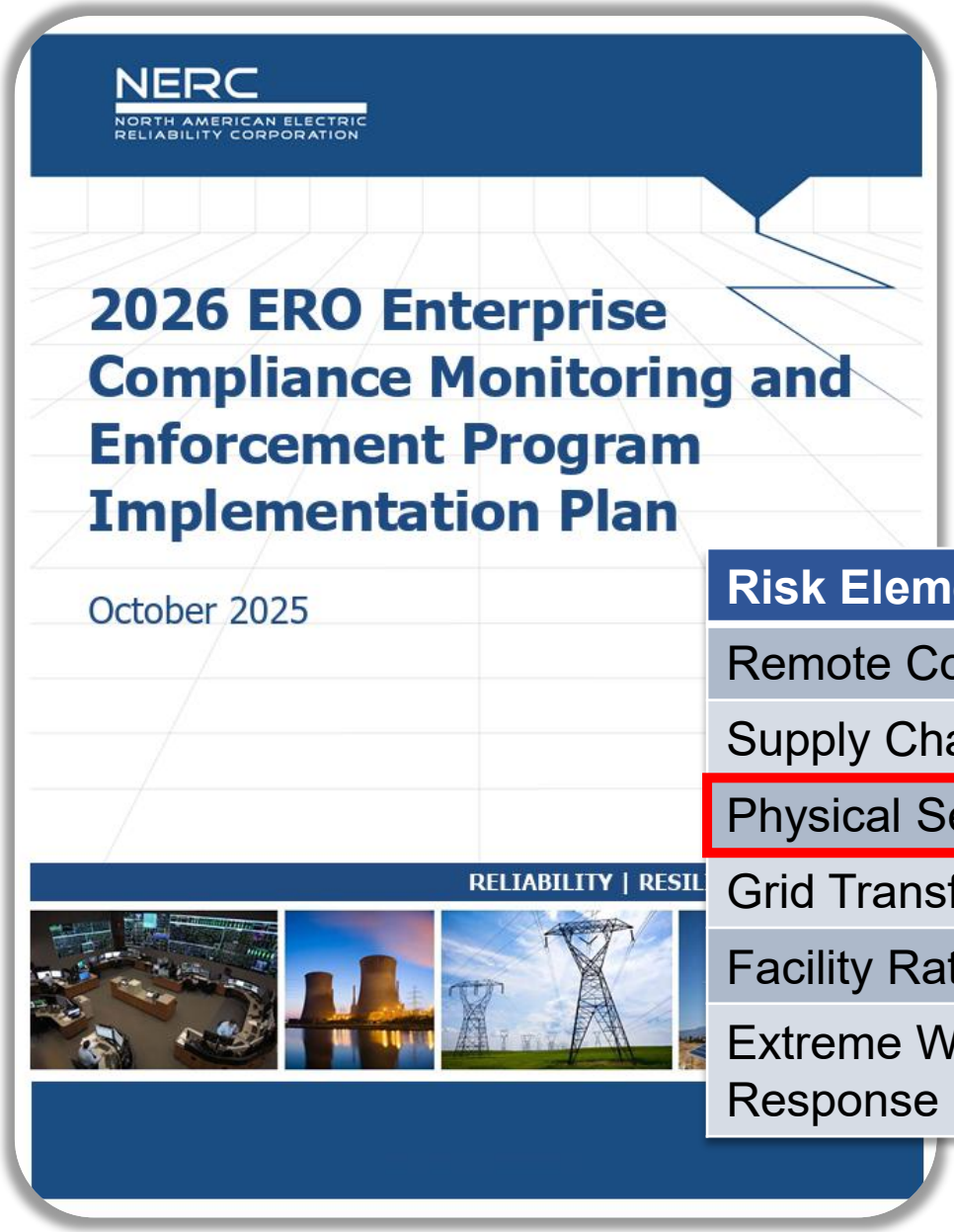
CIP-003-9 R2, Section 2: Physical Security

Josh Sily
CIP Cyber & Physical Security Analyst

November 6, 2026

Risk Focus & CMEP IP Risk Factors





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

Risk Element Areas of Focus: Physical Security

CIP-003-9 R2, Section 2: Physical Security

Table 4: Physical Security			
Rationale	**Standard**	**Req**	**Entities for Attention**
Mitigate risks to the reliable operation of the BES as the result of increased Physical Security events related to low impact assets.	CIP-003-8 CIP-003-9 (effective 4/1/2026)	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

CIP-003-9 R2 – Physical Security



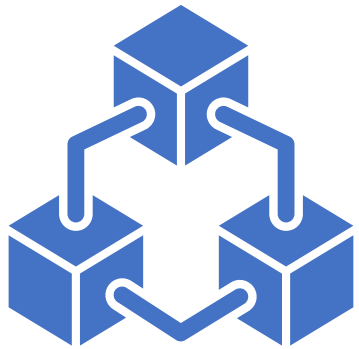
R2: Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.

CIP-003-9 R2 Attachment 1 Section 2

Attachment 1: Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Section 2: Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

CIP-003-9 R2 – Physical Security



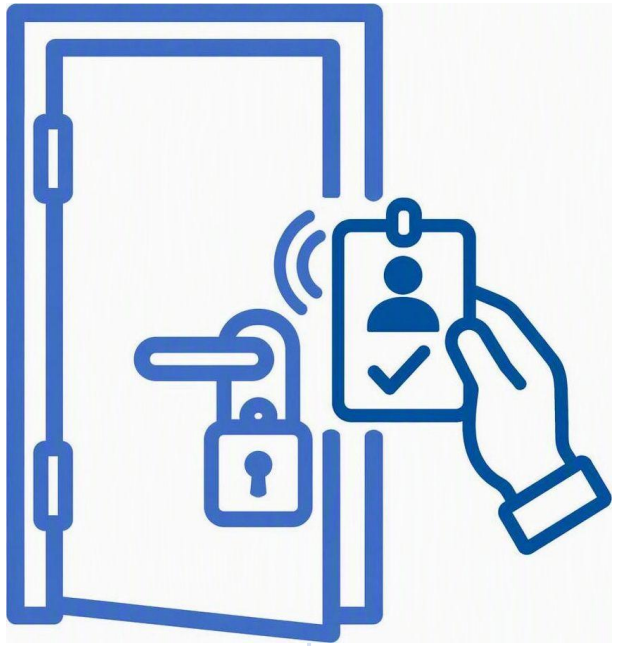
Control Physical Access to:

- Asset containing a low impact BES Cyber System
- Low impact BES Cyber System within the asset
- Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for section 3.1, if any

Examples of Physical Security Controls

BES Asset Level Controls	Low Impact BCS Location Physical Security Controls
• Physical barriers • Gates and physical access control • On-site security guards • Warning signs • Lighting and motion sensors • Closed-circuit television (CCTV cameras) • Intrusion detection system (IDS) (alarm systems) • Operational and procedural controls	• Doors and locks • Physical Access Control System (PACS) • Authentication systems • Physical intrusion detection systems (IDS) • Video management systems (VMS)

CIP-003-9 R2, Section 2: Site Evaluation









Best Practices

- Key Management
- Periodic Walkdowns
- Multiple Independent Controls

Resources

Physical Security Professional (PSP)

NIST SP 800-53 | NIST

Cybersecurity Framework 2.0 | NIST

Home Page | CISA



TEXAS RE
Ensuring electric reliability for Texans