Impact to Reliability

Ensure entities identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.
Disclaimer

The information contained in this presentation is drawn from our current understanding of this Standard and its Requirements as of the presentation date.

The WECC audit approach and information contained within this presentation is subject to change based on future guidance.
It’s about physical security.

Unlike most CIP Standards, CIP-014-2 is objective based, rather than prescriptive in nature. Perhaps subtle, it represents a significant shift to focus on an outcome rather than specific and defined measures.
Framing the Discussion

Congressional Research Service Report (R45135) March 19, 2018 Conclusion;

Therefore, although it is probably accurate to conclude that, based on the objectives of the CIP-014 standards, the U.S. electric grid is more physically secure than it was five years ago, it has not necessarily reached the level of physical security needed based on the sector’s own assessments of risk. Bulk power physical security remains a work in progress. As CIP-014 implementation and other physical security initiatives proceed, Congress may seek to maintain its focus on the power sector’s overall progress, not only on short term compliance with NERC’s security standards, but also on structural changes supporting physical security as a priority far into the future.

NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?  
https://fas.org/sgp/crs/homesec/R45135.pdf
Do’s and Don’t’s

• Do – Aim high! Nobody wants to explain the rationale for doing little or nothing after something bad happens.
• Do – Stick to the intent. It’s about physical security. Overanalyzing the standard word-for-word, or seeking minimal compliance misses the objective and is a waste of time and resources.
• Do – Engage top-notch industrial physical security practitioners with demonstrable examples of effective security solutions in the BES. Familiarity, proximity, experience, titles and certifications don’t always lead to a quality, effective solution.
Do’s and Don’t’s cont.

- Do – Connect the dots. Identified risk -> vulnerability -> protection solution(s) -> effective implementation. Trust but verify, and Repeat
- Do – Ensure 3rd party reviewers assess the security posture before, during and after plan execution. These reviews add no value if they assess compliance rather than security, offer little or no critical analysis or recommendations, or simply tell you what they think you want to hear.

Excerpt: Colin Powell – A Leadership Primer

Xerox's Barry Rand was right on target when he warned his people that if you have a yes-man working for you, one of you is redundant.
Successful Approaches

Requirement

• R4 Excerpt; “conduct an evaluation of the potential threats and vulnerabilities of a physical attack”

• R4.1 Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

Recommended Approach

• Use established processes such as CARVER and/or Design Basis Threat. All hazard analysis often loses specificity to this standard.

• Each asset may share a common purpose, but does not share identical threats or vulnerabilities. Define and document each site as if it were the only one.
A ring is a ring is a ring, right? They’re both pretty and they both get the job done, right? Not necessarily!
A Closer Look

Take a closer look

NO, Really Close

Just like evaluating a diamond, you have to look with the right knowledge, the right tools, the right attention to detail, the right certifications and the right passion for **objective unbiased evaluation**.
Success Approaches, Cont.

Requirement

• R4.2 Excerpt; “Prior history of attack on similar facilities”

• R4.3 Excerpt; “intelligence or threat warnings received from sources”

Recommended Approach

• Use established resources and peer utilities to create a well-informed macro and micro view of your threat landscape.

• Most programs assume bad things won’t happen. Flip the perspective, assume some things will, and plan accordingly.
Success Approaches, Cont.

**Requirement**
- R5 Excerpt; “develop and implement a documented physical security plan(s)”

**Recommended Approach**
- Resources engaged in this task should be as inclusive as possible. For example, there should representation from facilities, project management, substation engineering, transmission planning, IT/OT support, compliance staff and most importantly, industrial physical security practitioners.
Success Approaches, Cont.

Requirement

- **R5.1** 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.

Recommended Approach

- This is the heart of CIP-014-2. For each threat, answer these questions. Who, What, When, Where, Why and How. Before, during and after each potential scenario unfolds.
Define the problem, critically assess in-place and planned measures for effectiveness. Where lacking, design, deploy and validate effective security solutions.
Successful Approaches, Cont.

**Requirement**

- R5.2 Law enforcement contact and coordination information.

- R5.3 A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

**Recommended Approach**

- Engage early and often. Familiarity increases speed. Speedy effective response with an eye toward neutralization is the goal.

- Endeavor to remediate top threats and vulnerabilities ASAP. The activity timeline to completion should be commensurate with complexity.
Successful Approaches, Cont.

**Requirement**
- R5.4 Provisions to evaluate evolving physical threats, and their corresponding security measures
- R6 Excerpt; unaffiliated third party review

**Recommended Approach**
- Seek out evolving threats from the most credible sources, develop roles, responsibilities and solutions to address the dynamic landscape.
- Be suspicious of any assessment that tells you everything is perfect.
Common Pitfalls

• It’s in-scope, but it’s not really critical
• Missing implementation timeline deliverables
• Boilerplate TVAs and security plans
• Dissecting the standard word-for-word rather than meeting the objective
• Aiming for compliance rather than security
• “Nothing will happen to us”
• “We accept the risk(s)”
Common Pitfalls, Cont.

• Little if any analysis of the assets that comprise the site function or the unique threats and solutions appropriate to protect them collectively and individually

• Over reliance on grid resiliency measures. These measures are absolutely encouraged, but in the context of physical security, do not tend to provide demonstrable means to deter, detect, delay, assess, communicate and respond to physical threats

• 3rd party reviewers providing no value to the process
WECC Audit Approach:

WECC auditors will review an entity’s documentation pursuant to R4 Threat and Vulnerability and R5 Physical Security Plan as well as on-site performance testing to verify plan implementation. Auditors will review both resiliency and security measures outlined in R5 documentation. The measure of compliance, regardless of the application of these two approaches, will be a verifiable solution or solution(s) that collectively deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities.
Is Close Enough, Good Enough?

Dogbert Consults

I'll teach you the best practices of companies that have nothing in common with yours.

Those practices will fit your company like a foot in a glove.

Close enough.
Pop Quiz!

What is the purpose of CIP-014-2?

To identify and **protect** Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a **physical attack** could result in instability, uncontrolled separation, or Cascading within an Interconnection.
Beyond the Minimum
Tell Us Your Story!
Detect, Delay, Respond

Figure 2: Relationship between detecting, delaying and responding to a perimeter security breach

- Breach of perimeter
- Breach zone
- Access to asset
- Exit

Time needed by an adversary = delay achieved by physical security measures

Time needed by physical security systems

Safety margin

Detected
Dispatch response

Intercept adversary

Detection and assessment of breach