NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC/NERC Physical Security Technical Conference Agenda

August 10, 2023 | 9:00 a.m. - 4:30 p.m. Eastern
Hybrid Meeting

NERC Atlanta Office
3353 Peachtree Road NE, Suite 600 – North Tower
Atlanta, GA 30326

Welcome and Opening Remarks (9:00-9:12 am) (NERC and FERC)

NERC Antitrust Compliance Guidelines and Commission Staff Disclaimer (9:12-9:15 am) (NERC and FERC)

Agenda

Introduction and Background (9:15-9:30 am) (NERC and FERC)

Commission and NERC staff will provide background information relevant to discussion during the technical conference, including on Reliability Standard CIP-014-3, the current physical security landscape, recent Commission activities on physical security, and the NERC report filed with the Commission in April.

Reference and Resource Documents:

- FERC Order No. 802
- FERC Order Directing Report – December 15, 2022
- Reliability Standard CIP-014-3
- NERC Report on CIP-014-3
- FERC Notice of Technical Conference
- FERC Supplemental Notice – June 29, 2023
- FERC Supplemental Notice – July 27, 2023

Part 1: Effectiveness of Reliability Standard CIP-014-3

Part 1 of the technical conference will focus on Reliability Standard CIP-014-3, as it is enforced today as well as any potential revisions to the standard resulting in subsequent versions.

Panel 1 - Applicability (9:30-10:50 am) *Moderators: Olutayo Oyelade (FERC) and Kiel Lyons (NERC)*

This panel will explore the facilities subject to Reliability Standard CIP-014-3. While the NERC report filed with the Commission did not recommend revising the applicability section of the Standard at this time, the report determined that this could change based on additional information. Panelists will discuss whether the applicability section of Reliability Standard CIP-014-3 identifies the appropriate facilities to mitigate physical security risks to better assure reliable operation of the Bulk-Power System. Panelists will also discuss whether additional type(s) of substation configurations should be studied to determine risks and the possible need for required protections.

This panel may include a discussion of the following topics and questions:

1. Is the applicability Section of CIP-014-3 properly determining transmission station/substations to be assessed for instability, uncontrolled separation or cascading within the Interconnection? Specifically, are the correct facilities being assessed and what topology or characteristics should the applicable facilities have to be subject to CIP-014? For example, are there criteria other than those in Section 4.1.1 of CIP-014-3, such as connected to two vs. three other station/substations and exceeding the aggregated weighted value of 3000, changing the weighting value of the table in the applicability section, or including lower transmission voltages?

2. Given the changing threat landscape, are there specific transmission station/substation configurations that should be included in the applicability section of CIP-014-3, including combinations of stations/substations to represent coordinated attacks on multiple facilities? What would they be and why?

3. What other assessments (e.g., a TPL-001 planning assessment) may be used to identify an at-risk facility or group of facilities that should be considered for applicability under CIP-014-3? How stringent are those assessments? Describe any procedural differences between those other assessments and the CIP-014-3 R1 Risk Assessment. Should CIP-014-3 apply to entities other than those transmission owners to which 4.1.1 applies or transmission operators to which 4.1.2 applies?

4. Should potential load loss or generation loss be considered? If so, why, and how would potential impact be determined (e.g., how would potential load loss be determined in advance of running an assessment?)?

5. Should facilities that perform physical security monitoring functions that are not currently subject to CIP-014-3 (e.g., security operation centers) be covered by CIP-014-3 as well? If so, what criteria should be used?

Panelists:

- Mark Rice, Pacific Northwest National Lab
- Representative, Office of Cybersecurity, Energy Security, and Emergency Response (Department of Energy)
- Adam Gerstnecker, Mitsubishi Electric Power Products, Inc.
- Jamie Calderon, NERC
- Lawrence Fitzgerald, TRC Companies

Break (10:50-11:00 am)

Panel 2 - Minimum Level of Physical Protection (11:00 am-12:30 pm) *Moderators: Coboyo Bodjona (FERC) and Lonnie Ratliff (NERC)*

This panel will discuss the reliability goal to be achieved and based on that goal, what, if any, mandatory minimum resiliency or security protections should be required against facility attacks, e.g., site hardening, ballistic protection, etc. This panel will discuss the scope of reliability, resilience, and security measures that are inclusive of a robust, effective, and risk-informed approach to reducing physical

security risks. The panel will also consider whether any minimum protections should be tiered and discuss the appropriate criteria for a tiered approach.

This panel may include a discussion of the following topics and questions:

1. What is our reliability goal? What are we protecting against to ensure grid reliability beyond what is required in the current standards?
    a. What are the specific physical security threats (both current and emerging) to all stations/substations on the bulk electric system?
    b. As threats are continually evolving, how can we identify those specific threats?
    c. How do threats vary across all stations/substations on the bulk electric system? How would defenses against those threats vary?
    To what extent should simultaneous attacks at multiple sites be considered?
2. Do we need mandatory minimum protections? If so, what should they be?
    a. Should there be flexible criteria or a bright line?
    b. Should minimum protections be tiered (i.e., stations/substations receive varying levels of protection according to their importance to the grid)? How should importance be quantified for these protections?
    c. Should minimum protections be based on preventing instability, uncontrolled separation, or cascading or preventing loss of service to customers (e.g., as in Moore County, NC)? If minimum protections were to be based on something other than the instability, uncontrolled separation, or cascading, what burden would that have on various registered entities? If the focus is on loss of service, is it necessary to have state and local jurisdictions involved to implement a minimum set of protections?
    d. In what areas should any minimum protections be focused?
        i. Detection?
        ii. Assessment?
        iii. Response?
3. To what extent would minimum protections help mitigate the likelihood and/or reliability impact of simultaneous, multi-site attacks?

Panelists:

- Travis Moran, NERC/SERC
- Mike Melvin, Edison Electric Institute
- Kathy Judge, Edison Electric Institute
- Jackie Flowers, Tacoma Public Utilities
- Representative, American Public Power Association

Lunch (12:30-1:00 pm)

Part 2: Solutions Beyond CIP-014-3

Part 2 of the technical conference will focus on solutions for physical security beyond those requirements in Reliability Standard CIP-014-3.

Panel 3 - Best Practices and Operational Preparedness (1:00-2:30 pm) *Moderators: Joseph McClelland (FERC) and Bill Peterson (SERC)*

This panel will discuss physical security best practices for prevention, protection, response, and recovery. The discussion will include asset management strategies to prepare, incident training preparedness and response, and research and development needs.

This panel may include a discussion of the following topics and questions:

1. What is the physical security threat landscape for each of your companies? What best practices have been implemented to mitigate the risks and vulnerabilities of physical attacks on energy infrastructure?

2. What asset management and preparedness best practices have your member companies implemented to prevent, protect against, respond to, and recover from physical attacks on their energy infrastructure?

3. What research and development efforts are underway or needed for understanding and mitigating physical security risks to critical energy electrical infrastructure?

4. What research and development efforts, including the development of tools, would you like to see the National Labs undertake to assist your companies in addressing physical threats to your critical electrical infrastructure?

5. What do you need or would like to see from the energy industry to improve your ability and accuracy in addressing physical security risks to critical energy electrical infrastructure?

6. What best practices are in place to accelerate electric utility situational awareness of an incident and to involve local jurisdiction responders?

7. What can the federal and state regulators do to assist the energy industry in improving their physical security posture?

8. What training improvements can NERC and the Regional Entities implement to system operators to aid in real-time identification and recovery procedures from physical attacks?

9. What changes could be made to improve information sharing between the federal government and industry?

Panelists:

- Gupta Vinit, ITC Holdings Corp.
- Randy Horton, Electric Power Research Institute
- Craig Lawton, Sandia National Lab
- Michael Ball, Berkshire Hathaway Energy

- Thomas Galloway, North American Transmission Forum
- Scott Aaronson, Edison Electric Institute

Break (2:30-2:40 pm)

Panel 4 - Grid Planning to Respond to and Recover from Physical and Cyber Security Threats and Potential Obstacles (2:40-4:10 pm) *Moderators: Terry Clingan (FERC) and Ryan Quint (NERC)*

This panel will explore planning to respond to and recovery from physical and cyber security threats and potential obstacles to developing and implementing such plans. This discussion will focus on how best to integrate cyber and physical security with engineering, particularly in the planning phase. The panel will discuss whether critical stations could be reduced through best practices and how to determine whether to mitigate the risk of a critical station or protect it. Finally, the panel will consider the implications of the changing resource mix on vulnerability of the grid and its resilience to disruptions.

This panel may include a discussion of the following topics and questions:

1. How can cyber and physical security be integrated with engineering, particularly planning? What aspects of cyber and physical security need to be incorporated into the transmission planning process?

2. What modifications could be made to TPL-001 to bring in broader attack focus (e.g., coordinated attack)? What sensitivities or examined contingencies might help identify vulnerabilities to grid attacks?

3. Currently, if a CIP-014-3 R1 assessment deems a transmission station/substation as “critical” that station/substation must be physically protected. Are there best practices for reconfiguring facilities so as to reduce the criticality of stations/substations?

4. When prioritizing resources, how should entities determine which “critical” stations/substations to remove from the list and which to protect? If the project is extensive and may have a long lead time to construct, to what degree does the station/substation need to be protected during the interim period?

5. How will the development of the grid to accommodate the interconnection of future renewable generation affect the resilience of the grid to attack? Will the presence of future additional renewable generation itself add to or detract from the resilience of the grid to physical attack?

6. What are the obstacles to developing a more resilient grid? What strategies can be used to address these obstacles?
    a. Cost?
    b. Siting?
    c. Regulatory Barriers?
    d. Staffing/training?

Panelists:

- Ken Seiler, PJM Interconnection
- Tracy McCrory, Tennessee Valley Authority
- Daniel Sierra, Burns and McDonnel

Closing Remarks (4:10-4:30 pm)