e 6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket No. RD23-2-000]

Physical Security Technical Conference; Notice Inviting Post-Technical Conference Comments

On Thursday, August 10, 2023, the Federal Energy Regulatory Commission (Commission) and the North American Electric Reliability Corporation (NERC) convened a Physical Security Technical Conference to discuss physical security of the Bulk-Power System, including the adequacy of existing physical security controls, challenges, and solutions.

All interested persons are invited to file post-technical conference comments to address issues raised during the technical conference identified in the Final Notice of Joint Technical Conference issued on August 3, 2022. For reference, the questions included in the Final Notice are included below, and supplemental questions appear in *italics*. Commenters need not answer all of the questions but are encouraged to organize responses using the numbering and order in the below questions. Commenters are also invited to reference material previously filed in this docket but are encouraged to avoid repetition or replication of their previous comments. Comments must be submitted on or before **30 days** from the date of this Notice.

Comments, identified by docket number, may be filed electronically or paper-filed. Electronic filing through https://www.ferc.gov is preferred. Documents must be filed in acceptable native applications and print-to-PDF, but not in scanned or picture format. Instructions are available on the Commission's website: http://www.ferc.gov/docs-filing/efiling.asp.

Although the Commission strongly encourages electronic filing, documents may also be paper-filed. To paper-file, submissions sent via the U.S. Postal Service must be addressed to: Federal Energy Regulatory Commission, Office of the Secretary, 888 First Street NE, Washington, DC 20426. Submissions sent via any other carrier must be addressed to:

Federal Energy Regulatory Commission
Office of the Secretary
12225 Wilkins Avenue
Rockville, Maryland 20852.

For more information about this Notice, please contact:

Terrance Clingan (Technical Information)

Office of Energy Reliability
(202) 502-8823
Terrance.Clingan@ferc.gov

Leigh Anne Faugust (Legal Information)
Office of General Counsel
(202) 502-6396
Leigh.Faugust@ferc.gov

Dated: August 21, 2023.

Debbie-Anne A. Reese,
Deputy Secretary.

Post Technical Conference Questions

We are seeking comments on the topics discussed during the technical conference held on August 10, 2023, including responses to the questions listed in the Final Notice issued in this proceeding on August 3, 2023, as well as supplemental questions developed by Commission staff post-conference. The questions from the agenda and the supplemental questions are included below.

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

This panel explored 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 discussed 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 also discussed whether additional type(s) of substation configurations should be studied to determine risks and the possible need for required protections.

Please address the following 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-014-3? 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?

6. *Are there additional studies that could be performed – either by industry, the ERO Enterprise, the national labs, or others – that could be used to determine whether there are unidentified CIP-014 "critical" transmission stations and transmission substations? Are there additional studies that would help determine whether the applicability section of the standard requires expansion to identify those transmission substations/stations that if lost or rendered inoperable would result in instability, uncontrolled separation or cascading within an Interconnection.*

7. *How should extreme conditions be considered when identifying "critical" transmission substations/stations such as extended extreme weather events or disasters such as wildfires that weaken the resiliency of the Bulk-Power System?*

Panel 2: Minimum Level of Physical Protection

This panel discussed 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 discussed 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 also considered whether any minimum protections should be tiered and discuss the appropriate criteria for a tiered approach.

Please address the following 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?

4. *To what extent would the placement of basic security-related data recording devices and associated equipment at stations/substations (varying based on the criticality of the stations/substations as determined by the transmission owner) to allow for an assessment of damage and the collection of evidence in the event of an attack provide any security benefit? Such devices and equipment could possibly provide alarms in real time to operating centers or merely be reviewed on demand when a singular disturbance alarm is sent to an operating center.*

5. *Are there basic levels of protection that all Bulk-Power System facilities use, such as fencing? Would minimum improvements to these protections, such as adding better security requirements to the present public safety requirements, better deter attacks?*

6. *Given the increasing number and severity of physical security threats and perpetrated attacks:*

   i. Should transmission owners annually evaluate evolving physical threats and implement corresponding security measures for CIP-014 critical facilities?

   ii. What criteria should be considered in evaluating the impact of evolving threats and appropriate protections (e.g., criticality of load, likely duration of outage, location of station/substation)?

iii. *How should transmission owners prioritize security measures for facilities that are not CIP-014 critical facilities? For example, should transmission owners document and implement a tiered approach to protecting bulk electric system (i.e., 100 kV and above) stations and substations based on criteria characterizing the level of impact (high (i.e., CIP-014 critical), medium, or low), similar to CIP-002-5.1a?*

Panel 3: Best Practices and Operational Preparedness

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

Please address the following 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?

10. How do these best practices comport with the objectives of CIP-014-3?

Panel 4: Grid Planning to Respond to and Recover from Physical and Cyber Security Threats and Potential Obstacles

This panel explored planning to respond to and recovery from physical and cyber security threats and potential obstacles to developing and implementing such plans. This discussion focused on how best to integrate cyber and physical security with engineering, particularly in the planning phase. The panel discussed 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 considered the implications of the changing resource mix on vulnerability of the grid and its resilience to disruptions.

Please address the following 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?

7. How can transmission owners better work with state commissions on physical security? For example, are there opportunities to better work together as part

of approval processes for projects (e.g., applications for certificates of public convenience and necessity)?

8. *How can security protections be better integrated into the planning, engineering, and construction of projects that improve the security of the grid and overall performance and resilience, while keeping critical energy infrastructure information from being inappropriately released?*

[FR Doc. 2023-18336 Filed: 8/24/2023 8:45 am; Publication Date: 8/25/2023]