Background Information
On March 7, 2014, the Federal Energy Regulatory Commission (FERC) issued an order directing NERC to submit for approval, within 90 days of the order, one or more Reliability Standards to address physical security risks and vulnerabilities of critical facilities on the Bulk Power System (BPS).¹

In the order, FERC stated that the proposed Reliability Standard(s) should require entities to take at least the following three steps:

- Perform a risk assessment to identify facilities that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading failures on the BPS.
- Evaluate the potential threats and vulnerabilities to those identified facilities.
- Develop and implement a security plan designed to protect against physical attacks to those identified facilities based on the assessment of the potential threats and vulnerabilities to their physical security.

Additionally, FERC directed that the proposed Standard(s) should also: (1) include a procedure that will ensure confidential treatment of sensitive or confidential information; (2) include a procedure for a third party to verify the list of identified facilities and allow the verifying entity, as well as FERC, to add or remove facilities from the list of critical facilities; (3) include a procedure for a third party to review the evaluation of threats and vulnerabilities and the security plan; and (4) require that the identification of the facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. The proposed Physical Security Reliability Standard(s) must be filed with FERC by June 5, 2014.

In response to the order, NERC staff and the Standards Committee (SC) worked together in order to develop an action plan for meeting the June 5, 2014 filing deadline. The SC approved several waivers to facilitate meeting the required timelines and seated the Standard Drafting Team (SDT) on March 21, 2014.

¹ Reliability Standards for Physical Security Measures, 146 FERC ¶ 61,166 (2014).
This posting solicits comment on proposed Reliability Standard CIP-014-1 Physical Security. The proposed standard responds to the directives from the FERC order, and a summary of those directives with explanation of how the approach addresses them is available in the “Consideration of Issues and Directives” document on the project page.

You do not have to answer all questions below. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained. Due to the expected volume of comments, the SDT asks that commenters consider consolidating responses and endorsing comments provided by another.
Questions

1. **Applicability**: The applicability of proposed CIP-014-1 starts with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a “medium impact” rating. The drafting team did not modify these criteria in their use under CIP-014-1, as they have been previously approved by stakeholders, NERC, and FERC. The SDT sought to ensure that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1. The team determined that slightly modified criteria could possibly result in confusion in application. The drafting team considered several other alternatives to refine the scoping in the applicability section, such as a particular kV threshold in addition to the other criteria; however, after significant discussion, the team found no technical or reliability basis for providing such limitation. Importantly, by virtue of application of Requirement R1, the scope of the standard only applies to Transmission Owners that have Transmission stations and Transmission substations that meet the “medium impact” criteria from CIP-002-5.1, and their associated primary control centers. Furthermore, the standard drafting team expects many who are “applicable” to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In those cases, the entity only performs Requirements R1 through R2. When that results in a null set, Requirement R1 additionally provides that subsequent risk assessments may occur less frequently. Similarly, while Transmission Operators are also listed in the applicability section, by virtue of application of the requirements, only certain Transmission Operators that are notified under the standard’s Requirement R3 have obligations under the standard. Do you agree with the applicability section? If not, please provide specific recommendations, ensuring to articulate how your suggested approach would not limit the applicability in such a manner as to inadvertently miss a facility that should be covered under the standard as specified in the FERC order on physical security.

☐ Yes  ☒ No

Comments: The applicability of the draft standard should be expanded to include Planning Coordinators in addition to Transmission Owners and Transmission Operators. While NPCC agrees that TOs and TOPs simple application of the screening criteria to determine which facilities need analysis, they may not be able to conduct a complete analysis. The SDT should consider that Transmission Owners in some cases do not have the ability to conduct an analysis with a “wide area” view of consequences. Smaller TOs or TOPs only have an outside equivalent representation of the BES and could need help conducting their analyses. Consideration should be given to allow them to conduct the studies in conjunction with PCs.
2. **Requirements R1 through R3**: The first three requirements of CIP-014-1 require Transmission Owners to: (1) perform risk assessments to identify through transmission planning analysis those Transmission stations and Transmission substations that meet the “medium impact” criteria from CIP-002-5.1, and their associated primary control centers, that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; (2) arrange for a third party verification (as directed in the order) of the identifications; and (3) notify certain Transmission Operators of identified primary control centers that operationally control the identified and verified Transmission stations and Transmission substations. The requirements provide the periodicity for satisfying these obligations. Only an entity that owns or operates one or more of the identified facilities has further obligations in Requirements R4 through R6. If an entity identifies a null set after applying Requirements R1 through R2, the rest of the standard does not apply. Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security.

☐ Yes
☒ No

Comments: The Rationale Box for Requirement R2 stipulates that “‘unaffiliated’ means that the selected verifying entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission o(O)wner).” This conflicts with Requirement R2 Part 2.1 which lists “A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or An entity that has transmission planning or analysis experience” as those qualifications for an unaffiliated verifying entity. Clarification is needed that an Independent System Operator that has operating authority over an entity is eligible to be the unaffiliated verifying entity.
3. **Requirements R4 through R6**: The final three requirements of CIP-014-1 require (1) the evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified and verified according to the earlier requirements, (2) the development and implementation of a security plan(s) designed in response to the evaluation, and (3) a third party review of the evaluation and security plan(s) (as directed in the order). Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security.

- Yes
- ☒ No

**Comments**: Regarding Part 5.1, the requirement states that the security measures should be designed to deter, detect, delay, assess, communicate and respond to potential physical threats. NPCC suggests removing the obligation to ‘deter’ from this Part and establish a separate Part that addresses deterrence and very basic specifics regarding what constitutes deterrence. The new Part could describe how an entity should implement deterrence and consider some minimum auditable criteria; for example, Consider and Implement measures designed to deter potential physical threats including 1) perimeter control 2) motion detection 3) lighting 4) access control. In this manner the ambiguity surrounding the term ‘deter’ is eliminated.

Part 5.3 should allow flexibility to modify the time line. Suggest that Entities should 1) have a master Physical Security Plan; 2) have the flexibility to accomplish mitigation activities associated with the results of the vulnerability assessment, and 3) capture those mitigation plans under a separate mitigation plan (similar to the action plans for Cyber Assets vulnerability assessments) or include “associated modifications to the time line”.

4. Do you have input on other areas of the standard or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions. Please limit your response to 300 words or less.

- ☒ Yes
- No

**Comments**: It is NPCC’s expectation that RAI concepts will be applied to the operating and enforcement of this standard.